

# Contents

<b>1</b>	<b>Introducción a la versión en español del Manual de CryptoParty</b>	<b>15</b>
<b>2</b>	<b>Manual de CryptoParty</b>	<b>19</b>
	Prerrequisitos . . . . .	19
	Proceso de revisión de pares . . . . .	20
	Publicación . . . . .	20
	Licencia . . . . .	20
<b>3</b>	<b>Acerca de este libro</b>	<b>21</b>
<b>4</b>	<b>Prefacio</b>	<b>25</b>
<b>5</b>	<b>El manifiesto de la CryptoParty</b>	<b>29</b>
	¿Qué es una CryptoParty? . . . . .	32
	Sean amables los unos con los otros . . . . .	33
	Haga cosas . . . . .	33
<b>6</b>	<b>Cómo organizar una CryptoParty</b>	<b>35</b>
	Introducción . . . . .	35
	Antes de la fiesta . . . . .	37
	Lugares, infraestructura y comida . . . . .	37
	Página web . . . . .	39
	Difusión . . . . .	39
	Ángeles . . . . .	41

Materiales . . . . .	41
La fiesta . . . . .	42
Configurando la escena . . . . .	42
Discurso introductorio . . . . .	42
Temas . . . . .	44
Pidiendo ayuda . . . . .	45
Variaciones en el formato . . . . .	45
Roles . . . . .	46
Organizador . . . . .	46
<b>7 Orador</b>	<b>49</b>
Criptoángeles . . . . .	49
Meta-ángeles . . . . .	50
Construcción de una comunidad . . . . .	51
Encuentros nocturnos regulares . . . . .	51
Sesiones de entrenamiento . . . . .	51
Conferencias . . . . .	52
Recursos . . . . .	52
<b>8 Introducción a la versión en español</b>	<b>55</b>
<b>9 Consejos básicos</b>	<b>59</b>
Brevemente: . . . . .	59
Contraseñas . . . . .	60
Leyendo correos electrónicos en lugares públicos . . . . .	61
Almacenamiento malicioso . . . . .	62
Asegurando su comunicación . . . . .	62
DNSSEC & DANE . . . . .	64
Separación de cuentas . . . . .	65
Nota acerca del almacenamiento de correos electrónicos	65
<b>10 Tipos de correo electrónico</b>	<b>67</b>
Correo electrónico almacenado remotamente (“web-mail”) usando un navegador web . . . . .	68

---

Correo electrónico almacenado remotamente usando un programa o un navegador web . . . . .	68
Consideraciones de contexto . . . . .	70
Empleador/Organización . . . . .	70
Correos electrónicos & metadata . . . . .	71
Servidor de correo auto administrado . . . . .	71
Servicios de correo electrónico “gratuitos” . . . . .	71
Sin fines de lucro . . . . .	72
Notas sobre reenvío de correo electrónico . . . . .	72
<b>11 Temores</b>	<b>75</b>
Abusos al azar y robo por parte de hackers maliciosos . . . . .	78
Abuso dirigido, acoso y espionaje . . . . .	79
Cuando el cifrado funciona mal . . . . .	80
<b>12 Conexiones seguras</b>	<b>83</b>
¿Otras personas pueden leer mis mensajes mientras verifico mi correo electrónico? . . . . .	83
Notas . . . . .	84
<b>13 Correo electrónico seguro</b>	<b>87</b>
¿Qué software puedo usar para cifrar mi correo electrónico? . . . . .	88
<b>14 Consejos básicos</b>	<b>89</b>
Brevemente: . . . . .	89
Su navegador habla de usted por detrás suyo . . . . .	90
Los sitios web pueden rastrear por dónde usted navega . . . . .	90
Búsqueda online de información acerca de usted mismo . . . . .	91
Más ojos de los que usted puede ver . . . . .	92
Su derecho a permanecer en el anonimato . . . . .	93
<b>15 Temores</b>	<b>95</b>
Redes sociales - ¿cuáles son los peligros? . . . . .	95
¿Quién puede robar mi identidad? . . . . .	97

Redes inalámbricas . . . . .	97
El caché del navegador web . . . . .	98
Asegurando su línea . . . . .	98
¿Puedo meterme en problemas por usar Google con cosas raras? . . . . .	99
¿Quién mantiene un registro de mi navegación? . . . . .	99
¿Puedo esconderme de ellos? . . . . .	99
¿Cómo hacer para no revelar mi identidad? . . . . .	100
¿Cómo evitar ser rastreado? . . . . .	100
<b>16 Qué sucede cuando usted navega</b>	<b>101</b>
Una topografía suya: huellas . . . . .	103
¿Puede un sitio web malicioso apoderarse de mis cuentas? . . . . .	108
<b>17 Seguimiento</b>	<b>111</b>
¿Cómo lo siguen? . . . . .	112
¿Cómo puedo evitar el seguimiento? . . . . .	113
¿Cómo puedo ver quién me está siguiendo? . . . . .	123
Una palabra de advertencia . . . . .	123
<b>18 Anonimato</b>	<b>125</b>
Introducción . . . . .	125
Proxy . . . . .	126
Tor . . . . .	128
<b>19 VPN</b>	<b>131</b>
<b>20 Publicaciones anónimas</b>	<b>135</b>
Distintos no . . . . .	137
<b>21 Correo electrónico anónimo</b>	<b>141</b>
Envío de mensajes por medio de cuentas de correo electrónico desechables . . . . .	141
¡Sea cuidadoso con lo que dice! . . . . .	143

---

<b>22 Compartir archivos</b>	<b>145</b>
BitTorrent . . . . .	148
SoulSeek . . . . .	151
I2P . . . . .	153
<b>23 Llamadas seguras</b>	<b>155</b>
iOS - Instalando Signal . . . . .	156
Android - Instalando RedPhone . . . . .	156
Android . . . . .	157
<b>24 Usando Thunderbird</b>	<b>159</b>
Instalación de Thunderbird en Windows . . . . .	160
Instalación de Thunderbird en Ubuntu . . . . .	165
Instalación de Thunderbird en Ubuntu 12.04 o posteriores . . . . .	165
Instalación de Thunderbird en Mac OS X . . . . .	166
Usando Thunderbird por primera vez . . . . .	170
<b>25 Configuración de cuentas seguras</b>	<b>171</b>
Requisitos de configuración . . . . .	172
Preparación de una cuenta de Gmail para usar con Thunderbird . . . . .	173
Configurar Thunderbird para usar SSL / TLS . . . . .	173
Configuración manual . . . . .	176
Finalizando la configuración, diferentes métodos de cifrado . . . . .	180
De regreso a las pantallas de configuración . . . . .	180
<b>26 Parámetros adicionales de seguridad</b>	<b>181</b>
Configuración de correo basura . . . . .	182
Alerta y detección de estafas . . . . .	184
Integración con el antivirus . . . . .	184
Establezca una contraseña maestra . . . . .	187
Controles adaptables para correo basura . . . . .	191

<b>27 Introducción al cifrado de correo electrónico (PGP)</b>	<b>195</b>
Uso de un par de claves para cifrar su correo electrónico	197
Envío de mensajes cifrados a otras personas: usted necesita sus clave públicas . . . . .	198
Recepción de mensajes de correo electrónico de otras personas: ellos necesitan su clave pública . . . . .	198
Conclusión: el cifrado de mensajes requiere la distribución de las claves públicas . . . . .	198
<b>28 Instalación de PGP en Windows</b>	<b>201</b>
Instalación de PGP (GPG) en Microsoft Windows . . . . .	201
Instalación con la extensión Enigmail . . . . .	203
Pasos para la instalación . . . . .	204
<b>29 Instalación de PGP en OSX</b>	<b>209</b>
Comenzando . . . . .	209
Descarga e instalación del software . . . . .	210
Instalación de Enigmail . . . . .	217
<b>30 Instalación de PGP en Ubuntu</b>	<b>221</b>
<b>31 Instalación de GPG en Android</b>	<b>223</b>
APG . . . . .	224
Cómo habilitar GPG en correos electrónicos en Android: K-9 Mail . . . . .	224
<b>32 Creación de sus claves PGP</b>	<b>227</b>
Cifrado de archivos adjuntos . . . . .	238
Ingreso de una frase de paso . . . . .	239
Recepción de mensajes cifrados . . . . .	239
Envío y recepción de claves públicas . . . . .	240
Recepción de claves públicas y agregado de las mismas a su anillo de claves . . . . .	241
Uso de servidores de claves públicas . . . . .	246

---

Firma de un mensaje en particular . . . . .	253
Envío de mensajes cifrados a una destinatario en par-	
ticular . . . . .	255
Cifrado automático para destinatarios específicos . .	255
Verificación de mensajes entrantes . . . . .	264
Revocación de su par de claves GPG . . . . .	266
Qué hacer si pierde su clave secreta, u olvida la frase	
de paso . . . . .	266
Qué hacer si robaron su clave secreta, o si la misma	
está comprometida . . . . .	267
Recepción de un mensaje de revocación . . . . .	267
Preparándose para lo peor: copias de resguardo de sus	
claves . . . . .	268
Lecturas adicionales . . . . .	270
<b>33 Accediendo a Firefox en Ubuntu</b>	<b>273</b>
<b>34 Instalación en Mac OS X</b>	<b>275</b>
<b>35 Instalación de Firefox en Windows</b>	<b>281</b>
Usuarios de Windows Vista . . . . .	286
Problemas . . . . .	286
<b>36 Extensiones de Firefox</b>	<b>287</b>
HTTPS Everywhere . . . . .	288
Instalación . . . . .	290
Configuración . . . . .	291
Uso . . . . .	292
Si las redes bloquean HTTPS . . . . .	292
Añadir soporte para sitios adicionales en HTTPS Ev-	
erywhere . . . . .	295
Forzando conexiones seguras sobre servidor HTTPS .	296
Adblock Plus . . . . .	297
Comenzando con Adblock Plus . . . . .	298
Elección de una suscripción a un filtro . . . . .	298

Creación de filtros personalizados . . . . .	300
Habilitación y deshabilitación de AdBlock Plus para elementos o sitios web específicos . . . . .	301
Otras extensiones que pueden mejorar su seguridad . .	301
<b>37 Configuración de proxy</b>	<b>303</b>
Configuración del proxy por defecto . . . . .	304
<b>38 Uso de Tor</b>	<b>307</b>
Uso del paquete Tor para navegadores . . . . .	309
Descarga del paquete Tor para navegadores . . . . .	310
Ejecutando un repetidor o un puente . . . . .	310
Deshabilitación de búsqueda instantánea . . . . .	311
AdBlock para Chrome . . . . .	312
HTTPS Everywhere . . . . .	312
PrivacyFix . . . . .	312
<b>39 Manteniendo contraseñas seguras</b>	<b>313</b>
Extensión y complejidad de la contraseña . . . . .	313
Contraseñas seguras y fáciles de recordar . . . . .	314
Minimizar los daños . . . . .	314
El uso de un gestor de contraseñas . . . . .	315
La protección física . . . . .	315
Otras advertencias . . . . .	316
Instalación de KeePassX en Ubuntu . . . . .	316
Instalación de KeePass en Windows . . . . .	317
Instalación de KeePass en Mac OS X . . . . .	325
<b>40 Cifrado de contraseñas con un administrador</b>	<b>333</b>
Cifrado de contraseñas con KeePassX en Ubuntu . . .	334
Cifrado de contraseñas con KeePass en Windows . . .	340
Contraseñas cifradas con Keychain en Mac OSX . . .	347
<b>41 Obtención, configuración y prueba de una cuenta VPN</b>	<b>353</b>

---

Una cuenta de un proveedor comercial de VPN . . . . .	354
Configuración de su cliente VPN . . . . .	356
Configuración del cliente OpenVPN . . . . .	358
Advertencias...¡Cuidado! . . . . .	358
<b>42 VPN en Ubuntu</b>	<b>361</b>
Preparación del Network Manager para redes VPN . . .	361
Instalación de la extensión OpenVPN para Net- work Manager . . . . .	362
Configuración de una red OpenVPN . . . . .	367
Uso de su nueva conexión VPN . . . . .	372
<b>43 VPN en MacOSX</b>	<b>377</b>
Configuración . . . . .	377
Setup . . . . .	390
<b>44 Asegúrese que funcione</b>	<b>407</b>
<b>45 Instalando TrueCrypt</b>	<b>409</b>
Instalación en Ubuntu . . . . .	409
Instalación en OSX . . . . .	415
Instalación en Windows . . . . .	415
<b>46 Uso de TrueCrypt</b>	<b>421</b>
Crear un contenedor TrueCrypt . . . . .	421
Montando el volumen cifrado . . . . .	430
¿Qué significa esto? . . . . .	433
¡Recuerde desmontarlo! . . . . .	435
Nota acerca de los discos rígidos de estado sólido . .	445
Borrado seguro de datos en Windows . . . . .	445
Borrado seguro de datos en MacOSX . . . . .	448
Borrando el espacio libre . . . . .	448
Borrado seguro de archivos . . . . .	452
Borrado seguro de datos en Ubuntu . . . . .	454
Starting <i>Disks</i> . . . . .	461

Encrypting a device . . . . .	463
Using an encrypted device . . . . .	466
Introducción a la red OSTN . . . . .	467
CSipSimple . . . . .	468
<b>47 Configuración de mensajería instantánea cifrada</b>	<b>473</b>
Android - Instalación de Gibberbot . . . . .	473
iOS - Instalación de ChatSecure . . . . .	474
Ubuntu - Instalación de Pidgin . . . . .	474
OS X - Instalación de Adium . . . . .	475
Windows - Instalación de Pidgin . . . . .	475
Todos los OS - crypto.cat . . . . .	476
Archivos de registros de chat . . . . .	477
<b>48 Instrucciones para Debian Lenny y posteriores</b>	<b>481</b>
<b>49 Empezando con I2P</b>	<b>483</b>
<b>50 BitTorrent anónimos con I2PSnark</b>	<b>485</b>
Introducción . . . . .	486
Instalación . . . . .	487
Como usar OnionShare . . . . .	487
Ejemplos de cifrado . . . . .	498
¡Una advertencia! . . . . .	498
Cifrado histórico . . . . .	499
Cifrado moderno . . . . .	502
Criptografía cuántica . . . . .	505
Desafíos e implicaciones . . . . .	505
Administrador de contraseñas . . . . .	506
Agregador . . . . .	507
Análisis de amenazas . . . . .	507
Análisis de tráfico . . . . .	507
Ancho de banda . . . . .	508
Anonimato . . . . .	508
Archivo de registro . . . . .	508

---

ASP (proveedor de servicios de aplicaciones) . . . . .	509
Ataque por fuerza bruta . . . . .	509
Backbone . . . . .	509
Badware . . . . .	509
Bash (Bourne-again shell) . . . . .	510
BitTorrent . . . . .	510
Bluebar . . . . .	510
Bloqueo . . . . .	510
Caché . . . . .	511
Censorware . . . . .	511
Censura . . . . .	511
CGI (Interfaz de gateway común) . . . . .	511
Cifrado . . . . .	512
Cifrado completo de disco . . . . .	512
Cifrado de disco . . . . .	512
Clave pública . . . . .	513
Código (de cifrado) . . . . .	513
Confidencialidad directa perfecta (PFS) . . . . .	513
Cookie . . . . .	513
Criptografía . . . . .	514
Criptografía de clave pública/cifrado de clave pública	514
Clave privada . . . . .	514
Chat . . . . .	515
DARPA . . . . .	515
Descifrado . . . . .	515
Dirección IP (dirección del protocolo de Internet) . .	515
Dirección IP públicamente ruteable . . . . .	516
DNS (Sistema de nombres de dominio) . . . . .	516
Dominio . . . . .	516
Dominio de alto nivel con código de país (ccTLD) . .	517
Dominio de nivel superior (TLD) . . . . .	517
E-mail (correo electrónico) . . . . .	517
Escuchas ilegales . . . . .	518
Esquema . . . . .	518
Esteganografía . . . . .	518

Evasión . . . . .	519
Expresión regular . . . . .	519
Filtro . . . . .	519
Filtro de bajo ancho de banda . . . . .	519
Filtro de palabra clave . . . . .	520
Firefox . . . . .	520
Foro . . . . .	520
Frame (marco) . . . . .	520
FTP (Protocolo de transferencia de archivo) . . . . .	521
Fuga de DNS . . . . .	521
Gateway . . . . .	521
GNU Privacy Guard . . . . .	522
PGP . . . . .	522
Honeypot . . . . .	522
HTTP (Protocolo de transferencia de hipertexto) . . . . .	522
HTTPS (HTTP seguro) . . . . .	523
IANA . . . . .	523
ICANN . . . . .	523
Mensajería instantánea (IM) . . . . .	524
Intermediario . . . . .	524
Intercambio de archivos . . . . .	524
Interfaz común de gateway . . . . .	524
Interfaz de línea de comandos . . . . .	524
Internet . . . . .	525
IRC (Internet relay chat) . . . . .	525
ISP (Proveedor de servicio de internet) . . . . .	525
JavaScript . . . . .	525
KeePass, KeePassX . . . . .	525
Latencia . . . . .	526
Lista blanca . . . . .	526
Lista negra . . . . .	526
Malware . . . . .	527
Man in the middle . . . . .	527
Marcador . . . . .	527
Monitoreo . . . . .	528

---

Motor de difusión de archivos . . . . .	528
NAT (Traducción de dirección de red) . . . . .	528
Nodo . . . . .	529
Nodo abierto . . . . .	529
Nodo de enlace o intermedio . . . . .	529
Nodo de salida . . . . .	529
Nodo privado . . . . .	530
Nodo Psiphon . . . . .	530
Nodo sin salida . . . . .	530
Ofuscación . . . . .	530
Operador de red . . . . .	531
OTR (mensajes sin registro) . . . . .	531
Paquete . . . . .	531
Pastebin . . . . .	531
P2P . . . . .	532
PGP (Pretty Good Privacidad, <i>privacidad bastante buena</i> ) . . . . .	532
PHP . . . . .	532
POP3 . . . . .	533
Privacidad . . . . .	533
Protocolo . . . . .	533
Proxy Web . . . . .	533
Puente . . . . .	534
Puente Tor . . . . .	534
Puerto . . . . .	534
Remailer . . . . .	535
Router . . . . .	535
RSS (agregador de noticias) . . . . .	535
Salto (Hope) . . . . .	536
Screenlogger . . . . .	536
Script . . . . .	536
Script embebido . . . . .	537
Servidor de nombre raíz . . . . .	537
Servidor DNS . . . . .	537
Servidor proxy . . . . .	537

Shell (terminal, consola) . . . . .	538
Smartphone (teléfono inteligente) . . . . .	538
SOCKS . . . . .	538
Software de cadena de claves . . . . .	538
Spam . . . . .	539
SSH (shell seguro) . . . . .	539
SSL (Secure Sockets Layer, <i>capa de conexión segura</i> ) .	539
Subdominio . . . . .	540
Texto plano . . . . .	540
Texto sin formato . . . . .	540
TLS (Seguridad en capa de transporte) . . . . .	540
TCP/IP (Protocolo de control de transmisión sobre protocolo de Internet) . . . . .	540
Túnel . . . . .	541
Túnel DNS . . . . .	541
UDP (Paquete de datagramas de usuario) . . . . .	542
URL (localizador uniforme de recursos) . . . . .	542
Usenet . . . . .	542
VoIP (Protocolo de voz sobre Internet) . . . . .	543
VPN (red privada virtual) . . . . .	543
Webmail . . . . .	544
WHOIS . . . . .	544
World Wide Web (WWW) . . . . .	544
<b>51 La necesidad del software libre (o por qué es preferible al open source)</b>	<b>547</b>

# 1

## Introducción a la versión en español del Manual de CryptoParty

La siguiente es la versión en español del CryptoParty Handbook realizada por el Partido Pirata de Argentina. Antes de que siga leyendo, creemos necesario hacer algunas aclaraciones.

Hemos respetado fielmente el original traduciendo lo más literalmente posible al texto, algunas veces lo hemos logrado, otras no tanto. Por ejemplo, *click* puede traducirse por hacer *click*, hacer *clic*, *cliquear*, *presionar* o *pulsar*. La redundancia típica de estas palabras muchas veces en el mismo párrafo, incluso en la misma oración, hace que la traducción de la misma no sea uniforme. Por cuestión de estilo, la repetición de palabras en la misma oración no es muy agradable en castellano.

A determinadas palabras las hemos traducido por respeto al idioma y a sus expresiones locales. Aunque *email* es de amplio uso en Argentina, preferimos usar correo electrónico, ya que desconocemos la aceptación del original en inglés en la totalidad de las comunidades hispanohablantes.

**IMPORTANTE:** el manual está inmerso en una profunda cultura open source. En el apéndice podrá ver un artículo llamado ‘La necesidad del open source’. Prácticamente no hay mención a la importancia del software libre. Disentimos con esta postura. Sin embargo, por respeto al original, dejamos el artículo. Pero añadimos otro, que expresa ‘Por qué se debería usar software libre y no open source’.

Hemos cambiado ‘Linux’ por una expresión más adecuada, ‘GNU/Linux’. Para una explicación, consulte el artículo ¿Qué hay en un nombre?.

Ubuntu no es software completamente libre. No lo recomendamos, al igual que tampoco recomendamos Windows ni Mac OS. Todos los ejemplos de este manual se pueden aplicar perfectamente en Trisquel, que sí es totalmente libre. Para obtener una lista completa, consulte la guía de distribuciones GNU/Linux 100% libres.

¿Por qué no usar Ubuntu? Muy sencillo. Ubuntu provee repositorios específicos de software que no es libre, y Canonical promueve y recomienda explícitamente, bajo el nombre de Ubuntu, software que no es libre en algunos de sus canales de distribución. También ofrece la opción de instalar aplicaciones que no son libres. Además, la versión del kernel Linux que incluye contiene objetos binarios de firmware (blobs). Las políticas de marca registrada de Ubuntu prohíben la redistribución comercial de copias exactas, negando una importante libertad. Además, desde el mes de octubre de 2012, Ubuntu transmite datos personales acerca de las búsquedas realizadas por el usuario a un servidor de Canonical que restituye avisos publicitarios para comprar en Amazon. En sentido estricto, esto no influye

---

en el hecho de si Ubuntu es o no es software libre, sino que se trata de una violación de la privacidad de los usuarios. Además, anima a comprar en Amazon, una empresa involucrada en la DRM (Digital Restrictions Management, Gestión digital de restricciones) como así también en el maltrato de los trabajadores, autores y editores. La inclusión de esta publicidad involuntaria (adware) es uno de los raros casos en que un programador de software libre persiste en conservar una funcionalidad maligna en su versión de un programa.

Bueno, usted decide. Nuestro consejo es que use software libre, no open source (y menos software privativo). A partir de aquí, la traducción completa del original en inglés.



# 2

## Manual de CryptoParty

<https://cryptoparty.org/wiki/CryptoPartyHandbook>

**Por favor, siéntase libre de hacer un fork de este repositorio. Añada y edite contenido. Responda a las solicitudes recibidas.**

Los comentarios y preguntas acerca del contenido del manual son más que bienvenidos, por favor envíelas usando un asunto nuevo y creando una solicitud.

## Prerrequisitos

Para dar formato al manual (PDF, LaTeX, etc...) se requiere lo siguiente: - GNU make - pandoc - pdflatex

En Ubuntu se pueden instalar con la siguiente línea de comandos:

```
sudo apt-get install build-essential pandoc texlive-full
```

## Proceso de revisión de pares

Todavía no se ha implementado un proceso de revisión por pares para el contenido ya existente en el manual, así como para futuras incorporaciones. Esperamos que el contenido esté completo para finalmente ser revisado de acuerdo a la investigación en seguridad hasta al día y las mejores prácticas.

## Publicación

El Manual de CryptoParty pretende ser - y lucir - profesional, por lo que debe ser empaquetado y publicado de manera adecuada con un buen motor de composición tipográfica. Si usted tiene algún conocimiento o experiencia con la publicación de libros y archivos de texto, por favor involúcrese

## Licencia

El contenido CryptoParty Manual está disponible bajo la licencia Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0).

© Todos los capítulos de los contribuyentes a menos que se indique lo contrario.

# 3

## Acerca de este libro

El Manual de CryptoParty nació como una sugerencia de Marta Peirano (<http://petitemedia.es>) y Adam Hyde (<http://booksprints.net>) después de realizar la primera CryptoParty de Berlín, el 29 de agosto del 2012. Julian Olivier (<http://julianoliver.com>) y Danja Vasiliev (<http://k0a1a.net>), coorganizadores de la CryptoParty de Berlín junto con Marta estaban muy entusiasmados con la idea, viendo la necesidad de contar con un libro práctico de fácil comprensión para usar en las próximas CryptoParties. Asher Wolf, creador del movimiento CryptoParty, fue invitado a participar con el incipiente proyecto.

Este libro se escribió en los 3 primeros días de octubre del 2012 en Studio Weise7, Berlín, rodeado por buena comida y un pequeño océano de café. Estuvieron involucradas en su creación unas 20 personas, algunas más que otras, unas cerca, y otras más lejos.

La metodología usada para escribir, Booksprint (<http://booksprints.net>), trata de minimizar los problemas que acarrea el proceso de publicación de las páginas creadas. La discusión cara a cara y la asignación dinámica de tareas fueron

una parte muy importante de la realización del trabajo, ¡como en toda CryptoParty!

Para la tarea de edición usamos la plataforma de escritura open source Booktype (<http://booktype.pro>), basada en la web (HTML5 y CSS), que nos ayudó enormemente a desarrollarlo en forma paralela con relativa facilidad. Asher también abrió un par de páginas TitanPad para obtener financiamiento público para los capítulos del Manifiesto y Cómo hacer una CryptoParty.

Combinado, se convirtió en el manual oficial de CryptoParty en la medianoche del 3 de octubre, GMT+1.

La carrera por el libro duró 3 días y la lista completa de colaboradores incluye a:

- Adam Hyde (facilitador)
- Marta Peirano
- Julian Oliver
- Danja Vasiliev
- Asher Wolf (<http://cryptoparty.org>)
- Jan Gerber
- Malte Dik
- Brian Newbold
- Brendan Howell] (<http://wintermute.org>)
- AT
- Carola Hesse
- Chris Pinchen (<http://chokepointproject.net/>)
- Arte de tapa a cargo de Emile Denichaud (<http://about.me/denichaud>)

Esta versión del manual ha sido movido a Github para editarlo en forma colaborativa. Encuéntrelo en <https://github.com/cryptoparty/handbook>. Si encuentra errores o partes que necesiten mejoras, cree una cuenta de GitHub y empiece a editarlo, comentarlo o cree nuevas secciones. Si necesita más in-

---

formación referida al uso de git y github, consulte <https://help.github.com/>.

### Créditos del Manual de CryptoParty

#### Facilitador:

- Adam Hyde

#### Equipo principal:

- Marta Peirano
- Asher Wolf
- Julian Oliver
- Danja Vasiliev
- Malte Dik
- Jan Gerber
- Brian Newbold
- Brendan Howell

#### Asistentes:

- Teresa Dillon
- AT
- Carola Hesse
- Chris Pinchen
- ‘LiamO’
- ‘l3lackEyedAngels’
- ‘Story89’
- Travis Tueffel

#### Migración a GitHub, empaquetado y mantenimiento:

- Yuval Adam
- Samuel Carlisle
- Daniel Kinsman
- petter
- Jens Kubieziel
- Uwe Lippmann
- Kai Engert

Imagen de portada:

- Emile Denichaud.

Traducción al español:

- gnu\_tesla@riseup.net

Otros manuales incluidos:

- <http://www.flossmanuals.net/bypassing-censorship>

Los manuales usados en la segunda mitad de este libro se basan en 2 libros impresos por FLOSS Manuals:

- “How to Bypass Internet Censorship” 2008 & 2010 Adam Hyde (Facilitador), Alice Miller, Edward Cherlin, Freerk Ohling, Janet Swisher, Niels Elgaard Larsen, Sam Tennyson, Seth Schoen, Tomas Krag, Tom Boyle, Nart Villeneuve, Ronald Deibert, Zorrino Zorrinno, Austin Martin, Ben Weissmann, Ariel Viera, Niels Elgaard Larsen, Steven Murdoch, Ross Anderson, Helen Varley Jamieson, Roberto Rastapopoulos, Karen Reilly, Erinn Clark, Samuel L. Tennyson, A Ravi
- “Basic Internet Security” 2011 Adam Hyde (Facilitador), Jan Gerber, Dan Hassan, Erik Stein, Sacha van Geffen, Mart van Santen, Lonneke van der Velden, Emile den Tex y Douwe Schmidt

El contenido del Manual de CryptoParty está cubierto por la siguiente licencia Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0).

- © Todos los capítulos de los contribuyentes a menos que se indique lo contrario a continuación.

# 4

## Prefacio

Este libro es un esfuerzo continuado y colaborativo basado en dos manuales FLOSS How to Bypass Internet Censorship y Basic Internet Security y editados colaborativamente en Github aunque se están investigando otras formas posibles de colaboración.

Su objetivo es brindar un recurso completo para la gente que quiera asistir u organizar una CryptoParty pero simplemente carece de experiencia o de la confianza para llevarla acabo. Todos los capítulos están escritos para ser consultados independientemente unos de otros.

Todos los contenidos del *Manual de la CryptoParty* están cubiertos por la licencia Creative Commons Attribution-ShareAlike 3.0 Unported (CC BY-SA 3.0). La lista de autores se encuentra en *Apéndice A: Contribuciones*. Por qué es tan importante la privacidad =====

La privacidad es un derecho humano fundamental. Está reconocida en muchos países como fundamental para la dignidad individual y para los valores sociales de libertad de asociación y de expresión. En pocas palabras, la privacidad es la frontera

que separa nuestra intimidad de la intrusión de la sociedad.

Los países difieren en la definición de la privacidad. En el Reino Unido, por ejemplo, las leyes acerca de la privacidad se remontan al siglo XIV cuando la monarquía inglesa creó leyes para proteger a las personas de curiosos y mirones. Estas regulaciones se refieren a la intrusión en la intimidad de las personas, donde ni siquiera el rey de Inglaterra podía ingresar al hogar de la persona más humilde sin su permiso. Con esta perspectiva, la privacidad se define en términos de espacio personal y propiedad privada. En 1880, los abogados estadounidenses, Samuel Warren y Louis Brandeis describieron a la privacidad como el “derecho a estar solo”. En este caso, la privacidad es sinónimo del derecho a la vida privada. En 1948, la Declaración Universal de los Derechos Humanos protegió en forma específica la privacidad territorial y de las comunicaciones, que posteriormente se convirtió en parte de las constituciones de todo el mundo. La Comisión Europea de Derechos Humanos y el Tribunal Europeo de Derechos Humanos también señalaron en 1978 que la privacidad incluye el derecho a establecer relaciones con los demás y desarrollar el bienestar emocional.

Hoy en día, una faceta cada vez más importante de la vida privada son los datos personales que proporcionamos a las organizaciones, tanto online como offline. Cómo utilizan nuestros datos personales y cómo acceden a ellos es una temática que domina el debate sobre las leyes que rigen nuestro comportamiento y la sociedad. Esto, a su vez, tiene efectos en cadena sobre los servicios públicos a los cuales accedemos y cómo las empresas interactúan con nosotros. Incluso tiene efectos sobre cómo nos definimos. Si la privacidad está referida acerca de los límites que determinan a quién le damos permiso de vernos y seguir los aspectos de nuestras vidas, entonces la cantidad y tipo de información personal recopilada, procesada y diseminada es de suma importancia para nuestras libertades civiles fundamentales.

---

Un argumento oido a menudo, cuando se tratan las cuestiones de la privacidad y el anonimato, sigue la linea de, “Yo sólo hago cosas aburridas. Nadie va a estar interesado en eso de todos modos”, o “no tengo nada que ocultar”. Ambas argumentos son fácilmente rebatidos.

En primer lugar, una gran cantidad de empresas están muy interesados en estas cosas aburridas que usted hace porque ellos tienen la oportunidad de ofrecer “excelentes” productos adecuados a sus intereses. De esta manera, su publicidad se vuelve mucho más eficiente - son capaces de adaptarla específicamente a las necesidades asumidas y a los deseos. En segundo lugar usted tiene mucho que ocultar. Tal vez no lo exprese explícitamente en los mensajes que envíe a sus amigos y colegas, pero su navegación por la web - si no está protegida por las técnicas expuestas en este libro - les dirá mucho acerca de las cosas que usted quisiera mantener en secreto: una antigua pareja que usted busca a través de Google, las enfermedades que investiga o las películas que ve son sólo algunos ejemplos.

Otra consideración es que sólo porque usted no tenga algo que ocultar en este momento, no significa que no lo tenga que hacer en el futuro. Reunir todas las herramientas y habilidades necesarias para protegerse de la vigilancia requiere práctica, confianza y un poco de esfuerzo. Estas son cosas que podría no ser capaz de lograr y configurar justo cuando más lo necesite aunque no sea un espía. Un obsesionado, un acosador persistente, por ejemplo, es suficiente para alterar mucho su vida. Cuanto más fielmente siga las sugerencias de este libro, estos ataques tendrán menor impacto sobre usted. Las empresas también pueden acechar demasiado, encontrando más y más maneras de llegar a su vida diaria a medida que el uso de las redes de computadoras en sí mismo se profundiza.

Por último, la falta de anonimato y la privacidad puede que no le afecte, pero sí a toda la gente de su entorno. Si un tercero,

como su proveedor de servicios de Internet, lee su correo electrónico, también se viola la privacidad de todas las personas de su libreta de direcciones. Este problema se empieza a ver aún más dramáticamente cuando nos fijamos en los problemas de los sitios web de redes sociales como Facebook. Cada vez es más común ver fotos cargadas y etiquetadas sin el conocimiento o permiso de las personas afectadas.

Mientras lo animamos a ser políticamente activo para mantener su derecho a la privacidad, hemos escrito este libro con el fin de capacitar a las personas que sienten que el mantenimiento de la privacidad en Internet es también una responsabilidad personal. Esperamos que estos capítulos le ayuden a llegar a un punto donde puede sentir que tiene algo de control acerca de cuánto saben de usted otras personas. Cada uno de nosotros tiene el derecho a una vida privada, el derecho a explorar, buscar y comunicarse con los demás como uno desee, sin tener que vivir con el temor de miradas indiscretas.

# 5

## El manifiesto de la CryptoParty

**“El hombre no es él mismo cuando habla en nombre propio. Dale una máscara y te dirá la verdad.” - Oscar Wilde**

En 1996, John Perry Barlow, cofundador de la Electronic Frontier Foundation (EFF), escribió “Una declaración de independencia del ciberespacio”. Extrajimos los párrafos siguientes:

El ciberespacio consiste en transacciones, relaciones y opiniones en sí mismo, formando una onda estacionaria en la telaraña de nuestras comunicaciones. El nuestro es un mundo que está en todas partes y en ninguna a la vez, pero no está donde viven los cuerpos.

Estamos creando un mundo al cual todos pueden entrar sin privilegios o prejuicios debidos a la raza, el poder económico, la fuerza militar, o el lugar de nacimiento.

Estamos creando un mundo donde cualquiera, en cualquier sitio, puede expresar sus creencias, sin importar lo singulares que sean, sin miedo a ser coac-

cionado al silencio o el conformismo.

Dieciséis años pasaron, e Internet ha cambiado nuestra forma de vivir. Nos ha proporcionado el conocimiento combinado de la humanidad en la punta de nuestros dedos. Podemos establecer nuevas relaciones y compartir nuestros pensamientos y nuestras vidas con amigos de todo el mundo. Podemos organizarnos, comunicarnos y colaborar de formas que nunca nos hubiésemos imaginado posibles. Este es el mundo que queremos legar a nuestros hijos, un mundo con una Internet libre.

Desafortunadamente, no toda la visión de John Perry Barlow se ha cumplido. Sin acceso al anonimato online, no podemos librarnos de los privilegios ni de los prejuicios. La libre expresión no existe sin privacidad.

Los problemas que enfrentamos en el siglo 21 requieren que la humanidad trabaje junta. Los problemas que enfrentamos son serios: cambio climático, crisis energética, censura de los estados, vigilancia masiva y guerras sin fin. Debemos ser libres para comunicarnos y asociarnos sin miedo. Debemos apoyar los proyectos de software libre y de código abierto que nos ayuden a incrementar el conocimiento común de tecnologías de las cuales todos dependemos, por ejemplo, <http://opensourceecology.org/wiki> ¡Contribuya!

Para ejercer nuestro derecho a la privacidad y al anonimato online, necesitamos soluciones creadas mediante colaboración, abierta y distribuida, revisadas por pares. Las CryptoParties proporcionan la oportunidad de conocer y aprender a utilizar estas soluciones para darnos todos los medios necesarios para hacer valer nuestro derecho a la privacidad y al anonimato online.

1. Todos somos usuarios, luchamos por el usuario y nuestra misión es fortalecerlo. Afirmamos que los pedidos de los usuarios son la razón de existir de las computadoras. Con-

---

fiamos en la sabiduría colectiva de los seres humanos, no en los proveedores de software, corporaciones o gobiernos. Rechazamos los grilletes de los gulags digitales, montados sobre los intereses vasallos de los gobiernos y las corporaciones. Somos los ciberpunks revolucionarios.

2. El derecho al anonimato personal, a los seudónimos y a la privacidad son derechos humanos básicos. Estos derechos incluyen la vida, la libertad, la dignidad, la seguridad, el derecho a una familia, y el derecho a vivir sin temor o intimidación. Ningún gobierno, organización o individuo debe evitar que las personas tengan acceso a la tecnología que pone de relieve estos derechos humanos básicos.
3. La privacidad es el derecho absoluto del individuo. La transparencia es un requisito de los gobiernos y las empresas que actúan en nombre de las personas.
4. El individuo es el único dueño del derecho a su identidad. Sólo el individuo puede elegir que compartir. Los intentos coercitivos para obtener acceso a la información personal sin el consentimiento explícito es una violación de los derechos humanos.
5. Todas las personas tienen derecho a la criptografía y a los derechos humanos que las herramientas criptográficas involucran, independientemente de su raza, color, condición sexual, idioma, religión, opinión política o de otra índole, origen nacional o social, nacimiento, posición económica, política, jurídica o internacional del país o territorio en el que reside.
6. Así como los gobiernos deben existir sólo para servir a sus ciudadanos - así también, la criptografía debe pertenecer a gente. La tecnología no debe ser inaccesible para la gente.
7. La vigilancia no se puede separar de la censura y la esclavitud que implica. Ninguna máquina debe estar al servicio

de la vigilancia y la censura. La criptografía es una clave para nuestra libertad colectiva.

8. El código es discurso: es un lenguaje humano creado. Prohibir, censurar o bloquear la criptografía para que la gente no tenga acceso a ella es privar a los seres humanos de un derecho humano, la libertad de expresión.
  9. Aquellos que buscan detener la propagación de la criptografía se asemejan a los clérigos del siglo 15 que trataban de prohibir la imprenta, temerosos de que su monopolio del conocimiento fuera socavado. Fiesta como en el 31 de diciembre de 1983
- 

## ¿Qué es una CryptoParty?

*CryptoParty* es una iniciativa global, descentralizada, con el objetivo de introducir herramientas básicas de criptografía - tales como la red de anonimato Tor, la clave de cifrado pública (PGP/GPG), y OTR (Off The Record messaging) - al público en general.

La idea de una CryptoParty fue concebida como respuesta a la Australian Cybercrime Legislation Amendment Bill 2011 y su razón de ser es que leyes como estas se vuelven inútiles cuando todos cifran sus comunicaciones.

Las CryptoParties no tienen fines comerciales ni políticos, y son libres y abiertas para todos aquellos que sigan sus *principios guía*:

---

## **Sean amables los unos con los otros**

Las CryptoParties son eventos en donde las personas se sienten bienvenidas y seguras para aprender y enseñar sin importar sus conocimientos ni su nivel de experiencia. Todas las preguntas son relevantes, todas las explicaciones deberían estar dirigidas a las personas con menos conocimientos.

Esto también significa que toda forma de acoso u otro comportamiento que incomode a las personas no tiene cabida en las CryptoParties. De acuerdo a nuestra experiencia, estas situaciones (aunque no suceden muy a menudo) se deben más a ineptitud en el trato social que a malicia y pueden ser resueltas instando a las personas a ser más cuidadosas con sus comportamientos, pero la responsabilidad final recae sobre los organizadores de la CryptoParty quienes deben invitar a retirarse a aquellas personas que no adhieran a esta sencilla regla, Sean amables los unos con los otros. La concientización es la clave en este respecto.

## **Haga cosas**

En las CryptoParties suceden cosas porque las personas hacen cosas. Las experiencias de aprendizaje más sorprendentes e inesperadas suceden porque la gente hace que sucedan. Si no está seguro de lo que tiene en mente o de si otras personas están interesadas en ello haga lo siguiente: propóngalo de todas formas y fíjese si alguien tiene algo que decir. Si es demasiado tímido para proponerlo a toda la audiencia, diríjase a la persona más cercana a su lado.

A una escala más global, existe una lista de correo <global@cryptoparty.is> que está abierta a todas las preguntas y discusiones de todo tipo, también pueden encontrarse

listas de correo específicas para cada ciudad y país y otros recursos en <https://cryptoparty.in>.

Para una guía acerca de cómo organizar una CryptoParty por favor consulte el capítulo con el mismo nombre.

DIY, movimiento autoorganizado, inmediatamente se volvió viral, con una docena de CryptoParties autónomas organizadas en horas en ciudades a lo largo de Australia, EEUU, el Reino Unido, y Alemania.“](<http://en.wikipedia.org/wiki/CryptoParty>)

Actualmente, dieciséis CryptoParties se han realizado en una docena de países diferentes a nivel mundial, y muchos más están previstas. El uso de Tor en Australia se ha incrementado después de cuatro CryptoParties, y la CryptoParty de Londres tuvo que ser trasladada del Hackspace al campus de Google para acomodar el gran número de participantes ansiosos, con 125 asistentes y 40 personas en lista de espera. Del mismo modo, la CryptoParty de Melbourne despertó gran interés superando la capacidad del lugar - originalmente prevista para aproximadamente 30 participantes - cuando se presentaron más de 70 personas.

La CryptoParty ha recibido mensajes de apoyo de la Electronic Frontier Foundation, de AnonyOps, del informante de la NSA Thomas Drake, del ex editor central de WikiLeaks Heather Marsh, y del reportero de Wired, Quinn Norton. Eric Hughes, el autor hace veinte años de *Un manifiesto ciberpunk*, pronunció un discurso de apertura en la primera CryptoParty en Amsterdam.

# 6

## Cómo organizar una CryptoParty

### Introducción

CryptoParty es un movimiento comunitario global y descentralizado. Como tal, varía mucho según el lugar en donde se desarrolle. Este tutorial está escrito para poder brindarle algunas ideas acerca de qué es lo que funciona bien y qué no, pero todo como una acción directa: los planes no seon nada, la planificación es todo, y todo está bien siempre y cuando esté de acuerdo con los siguientes principios ([https://cryptoparty.in/guiding\\_principles](https://cryptoparty.in/guiding_principles)): sean amables unos con otros y hagan cosas.

Si prefiere el video sobre el texto: (<https://va.ludost.net/files/initlab/20140502cparty.mp4>) (grabado en initlab en abril del 2014).

O únase a nosotros en IRC (#cryptoparty.oftc.net) o la lista de correo [global@cryptoparty.is](mailto:global@cryptoparty.is)

Por favor, contáctese con nosotros a través de dichos canales de comunicación si tiene alguna duda o necesita ayuda.

Una CryptoParty no puede enseñarle todo lo que deba saber acerca de las computadoras y la seguridad en Internet en una tarde. El objetivo principal es derribar las barreras mentales que impiden que las personas piensen acerca de estos temas o los enfrenten a medida que aparecen en sus vidas, en artículos periodísticos, en blogs, en el ámbito educativo y memes. Existe una gran cantidad de información acerca de las computadoras y la seguridad en internet ahí afuera. Lamentablemente, muchas personas no se consideran capaces de procesar dicha información, y mucho menos de intentarlo. Esto es lo que nosotros queremos cambiar. Despejando el miedo a las cosas crípticas y técnicas (dos propiedades inherentes a todas las herramientas criptográficas) podrá continuar aprendiendo y enseñando a otros.

Con una CryptoParty usted creará un ambiente en donde personas de diferente formación se juntarán y aprenderán unas de otras. Por lo tanto, sería deseable incluir personas de diferente edad, género, nivel cultural y experiencia.

Con las puertas abiertas, la gente llega, busca un asiento y socializa. Una breve introducción inaugura oficialmente el evento y luego todos se dirigen a las mesas. Cada mesa debe cubrir un tema y la gente debe decidir que le gustaría aprender y/o enseñar.

Las personas se sentirán más cómodas si cuentan con el tiempo suficiente para socializar. Se sentirán más a gusto para formular preguntas. Esto sucederá en un ambiente adecuado. Preparar la escena es su tarea.

El discurso de apertura debería ser tan breve como sea posible (no más de veinte minutos) y debería dar un vistazo general acerca de qué se debería esperar (consulte el capítulo dedicado

---

a tal fin para más detalles). En algunas ciudades, también hay charlas. Funciona muy bien cuando la gente busca una introducción en profundidad. La mayoría de las veces querrán pasar a la acción rápidamente. Dependiendo del grupo podría ofrecer ambas opciones en habitaciones separadas.

Apenas concluya la introducción, la gente se debe dirigir a las mesas con el tema de su preferencia. No se procupe si todo luce algo caótico durante algunos minutos. Cada mesa abre con una introducción más específica antes de instalar, configurar o usar cualquier herramienta. Insista, aliente a que todos realicen preguntas todo el tiempo.

La capacidad de improvisar es muy útil en la CryptoParty como en todo aprendizaje en donde habitualmente surgen situaciones inesperadas.:-

Si todos trabajan se sorprenderá por la energía positiva, por el compromiso, concentración y diversión de la gente. Las mejores CryptoParties generalmente duran hasta bien entrada la noche aún después de un largo día (o semana) de trabajo.

La duración recomendada para una CryptoParty es de 3 a 5 horas.

Aquí hay una lista completa de cosas que hemos aprendido de las pasadas CryptoParties:

## **Antes de la fiesta**

### **Lugares, infraestructura y comida**

El público de una CryptoParty y su conducta general estarán condicionados en gran medida por el lugar en donde suceda todo. No importa si es un bar, un club, un centro social, una escuela, una universidad, una biblioteca, una sala de prens, una ONG

o una empresa: mientras sea de libre acceso y gratuita, y sin banderías políticas ni fines de lucro estará bien. Pero sea cuidadoso con las oficinas empresariales. Si tiene alguna duda, por mínima que sea, pregunte a otro organizador de CryptoParties por medio de la lista de correo local o global si ellos se sentirían cómodos realizando un evento en el lugar en cuestión.

Una cosa muy importante - posiblemente aún más que la electricidad e Internet - es la comida. Es casi imposible que alguien no se comporte amablemente después de una buena comida. Bueno, sí, generalmente usted querrá tener también electricidad y una buena conexión a Internet para ser capaz de brindarles a todos el software y la experiencia que vinieron a buscar.

Los criterios generales para tener un buen lugar son:

- debe ser acogedor
- tener bebidas
- idealmente, tener comidas
- tener sillas y mesas suficientes
- tener alargues y zapatillas eléctricas
- tener una conexión a Internet lo suficientemente rápida

Recuerde que su público mayormente no está familiarizado con la escena hacker.

Lugares adecuado puede ser:

- cafés
- espacios comunitarios
- bibliotecas
- escuelas
- universidades
- hacklabs
- clubes nocturnos
- cualquier lugar que le parezca

---

## Página web

Ya sea que hospede la página web de su CryptoParty en su propio servidor o use cryptoparty.in, asegúrese de poner al menos un enlace en nuestra página, ya que la CryptoParty es un esfuerzo global, colaborativo. y así otras personas podrán enterarse de su existencia y unírseles.

Algunos elementos que deberían tener son:

- un texto de bienvenida
- fechas de reuniones futuras
- lista de lugares
- información de contacto (preferiblemente correo electrónico)

Supongamos que su ciudad no posee página web. Cree una para la ciudad entera (por ejemplo, “<https://cryptoparty.in/ciudad-gotica>”). Aquí debería ir la información. Los lugares o las reuniones deberían tener subpáginas. Esto le permitirá a otros organizar reuniones sin tener que crear una segunda versión de la página de dicha ciudad.

Usted puede ayudar creando una página básica para ser copiada por otros, para que la ajusten a sus necesidades, y puedan brindarle su opinión para mejorarlala.

Por favor añada las fechas de sus reuniones en la lista global de fechas aunque no use la wiki como su sitio web principal. Ayúdenos a mostrar cuán global es el movimiento. Podrá encontrar un tutorial dedicado aquí <https://cryptoparty.in/parties/add-a-date>.

## Difusión

La difusión ayudará a dar a conocer su CryptoParty. Primero debe pensar en su público promedio. Deberían ser personas

que aún no han cifrado nada. Ellos conocen como encender una computadora pero no tienen conocimientos avanzados en el tema.

Comience de a poco. Dependiendo del número de ángeles disponibles probablemente no querrá cientos de asistentes a su CryptoParty. Los lugares tienden a venir con una comunidad. Si están interesados en hospedar una CryptoParty entonces su comunidad estará interesada en asistir a ella. Si logra que estén contentos ellos le dirán a sus amigos lo maravilloso que fue todo.

Anuncie la CryptoParty en la wiki, en las listas de correo, y en todos los canales relevantes que pueda, a saber:

- online
- listas de correo
- blogs
- redes sociales
- offline (consulte [github.com/cryptoparty/flyers](https://github.com/cryptoparty/flyers))
- folletos
- stickers
- posters
- boca a boca
- medios de comunicación locales

¿Podrá poner posters o folletos en algún sector del lugar? ¿Tendrá el lugar alguna lista de correo? Considere crear una lista de correo y cuentas en las redes sociales para su ciudad. Las listas de correo, Diaspora y Twitter suelen ser muy populares en la comunidad de la CryptoParty.

Conectarse con la comunidad global de la CryptoParty puede ser muy útil para aprender de las experiencias pasadas y retomarlas con nuevo impulso.

- listas de correo
- IRC

- 
- Twitter
  - Diaspora

## Ángeles

Decida qué tema le gustaría enseñar. Para ver cómo enseñan otros revise la lista de manuales. Las explicaciones deben estar dirigidas a los principiantes. Tenga esto siempre en mente. <https://www.level-up.cc/> tiene una sección específica acerca de cómo ser un mejor instructor.

No sea crítico, Respete las decisiones de la gente acerca de cuáles herramientas usar y cuánto comprometerse en su decisión de proteger su privacidad. No responda sus preguntas como si fueran estúpidas. Todas las preguntas son buenas.

Contacte al organizador y hágale saber lo que desea enseñar. Ayúdelo a planificar la CryptoParty. Cuantos más ángeles haya y cuanto más pequeños sean los grupos la experiencia será mucho mejor para todos los participantes. También debería hacerse de algo de tiempo para aprender de otros ángeles.

Lleve bolígrafos y papel a la CryptoParty para dibujar diagramas mientras explica cómo funciona algo.

## Materiales

Lista de cosas que debería tener a mano durante una CryptoParty:

- Formularios varios para las mesas
- folletos (CryptoParty o grupos similares)
- stickers
- memorias usb
- todo el software relevante descargado (y verificado en medida de lo posible)

- huellas y firmas digitales de Tor, Tails, PGP y otros proyectos.

## La fiesta

### Configurando la escena

Quizás sea la parte más importante. La fortaleza de las CryptoParties se basa en la unión de diferentes personas de las más diversas experiencias que se comprometen a aprender unos de otros. Pero también implica un desafío para que personas de diferentes opiniones “sean amables unas con otras”.

Un primer paso, aún antes de iniciar oficialmente la fiesta, es darle la bienvenida a cada persona y grupo a medida que lleguen y asegurarse que no se sientan solos o perdidos. Esto es especialmente importante cuando se demore el inicio, lo que sucede más a menudo de lo que debería, pero esto aplica a toda la reunión. Solo asegúrese de que todos sean amables unos con otros y hagan cosas (por ejemplo, tomar un te y charlar amigablemente). Derribe murallas.

### Discurso introductorio

Según nuestra experiencia es muy útil disponer de un plan general acerca de los temas potenciales a cubrir

El discurso introductorio inaugura oficialmente la CryptoParty. Dependiendo de su estilo propio, puede ser preferible ser realista o algo más osado. Pero sea breve (no más de 20 minutos) y no entre en detalles técnicos ya que eso es lo que hará cada grupo de aprendizaje individualmente.

---

Si prefiere mostrar un video, fíjese el video de introducción a la CryptoParty.

Los puntos potenciales a tratar pueden ser:

- Saludo y bienvenida
- Agradecimiento a la gente que cedió el lugar
- Sean amables unos con otros
- que es una CryptoParty
- movimiento global y descentralizado
- todos pueden ser parte de él
- un tema por mesa
- cada persona elige su tema
- advertencia de seguridad
- no existe el nivel de seguridad al 100% (ni online ni offline)
- usar cifrado es legal, pero no en todos los países
- la CryptoParty es para principiantes
- en segundo lugar, es para los periodistas, los activistas y hasta para los expertos (por ejemplo, [EFF] (<https://www.eff.org/> ), Tactical Tech, AccessNow)
- existe el prejuicio de que la criptografía es difícil
- la seguridad es un proceso
- no es un producto
- no es algo que usted instala
- es algo que usted hace
- software libre
- servicios descentralizados
- no controlados por una sola organización
- lista de temas presentados en una específica CryptoParty

No ofrezca una falsa sensación de seguridad, pero tampoco ate morece a la gente con todas las formas en que las cosas podrían empeorar. Algunas personas *quieren* escuchar todas las cosas que podrían empeorar y no son temerosas, pero usted necesitará discutir el tema individualmente con cada persona, no en un discurso introductorio.

## Temas

Esta lista solamente es una sugerencia. Los grupos de aprendizaje se formarán alrededor de estos temas y dependiendo del espacio disponible, de la cantidad de personas dispuestas a aprender y de la cantidad de personas dispuestas a conducir un grupo de aprendizaje podrán ser agrupados de forma más amplia o más específica.

Su oferta dependerá de los ángeles disponibles. Posteriores sugerencias se enlistarán en un [resumen de herramientas]<https://cryptoparty.in/learn/tools> ) separado. Todo es software libre y de código abierto. Y por supuesto, nos agradan también los servicios descentralizados.

- discusión y mesa de orientación
- cifrado de correo electrónico con PGP
- cifrado de mensajería instantánea con XMPP y [OTR]  
([https://es.wikipedia.org/wiki/Off\\_the\\_record\\_messaging](https://es.wikipedia.org/wiki/Off_the_record_messaging))
- navegación web anónima Tor
- plugins para mejorar la navegación privada
- seguridad en telefonía móvil (Android, iOS)
- cifrado de discos y archivos con VeraCrypt
- cifrado de discos con LUKS
- seguridad en contraseñas y su administración
- instalación de distribuciones GNU/Linux
- Tails (sistema operativo anónimo y seguro... no olvide decirle a la gente que lleve una memoria usb)

Una mesa de orientación y discusión debería tratar el tema de cuanta vigilancia es necesaria y por qué todos tenemos algo que ocultar. La mayoría de las personas no son exhibicionistas y valoran su privacidad. Por lo tanto piense en alguien curioso pero aún no convencido del beneficio de la criptografía.

En la mesa de discusión y orientación, deberá tratar con un

---

montón de preguntas inesperadas. Algunas pueden parecerles irrelevantes. No intente dirigir la conversación, responda todas las preguntas sin juzgarlas.

## Pidiendo ayuda

Siempre pida ayuda. Las CryptoParties no equivalen a trabajo duro individual. Si el estrés sobrepasa la diversión, deténgase un momento y vea que todo continúa mágicamente aún sin usted. Lo principal es invitar a la gente para que ayude. decirle que pueden ayudar y que su ayuda será muy apreciada. Para la CrptoParty en cuestión o para todas. Si ve gente que se presenta por tercera vez consecutiva, pregúntele si desea hospedar una mesa, si la gente habla acerca del bar en donde trabajan o la casa en donde viven, pregúntele si esos lugares son adecuados para una CryptoParty y si ellos pueden organizar una. Las oportunidades son innumerables.

## Variaciones en el formato

Las CryptoParties para un grupo específico pueden ayudar a reducir la barrera de “Este no es mi campo de experiencia, no comprenderé nada”. Considere organizar CryptoParties para periodistas, estudiantes, grupos específicos de activistas, etc. Aún, incluso considerando la preparación dedicada, todos los que quieran ayudar deben ser bienvenidos.

Si desea llegar a las personas que son demasiado tímidas para participar o si encontrar un lugar se hace muy difícil quizás querrá visitar gente en su lugar para lo que denominamos un “Cryptoparty en una hogar/en un living room”.

## Roles

Así como existen diferentes eventos, también hay diferentes roles en una CryptoParty. Esta sección resume todos los roles.

- organizadores
- oradores
- criptoángeles
- meta-ángelos

## Organizador

Como organizador de una CryptoParty, necesita hallar un lugar donde la gente se sienta cómoda. Debe mantenerse en contacto con la gente que administra el espacio y hallar una fecha adecuada para todos. Los lugares puede ser espacios comunitarios, cafés, bibliotecas, escuelas, universidades, hacklabs... y cualquier otro lugar acogedor y con suficiente cantidad de sillas, mesas, conexiones eléctricas y una buena conexión a Internet.

Debería ser cuidadoso de la difusión además del alcance de la palabras acerca de cuando y donde sucede la CryptoParty. La difusión tiene una sección separada (consulte más arriba).

Por último pero no por eso menos importante necesitará contar con una suficiente cantidad de personas para explicar las herramientas específicas y llevar adelante la CryptoParty con usted. Si usted tiene suficiente experiencia podrá sacarla adelante casi sólo y organizar a sus ayudantes (algunos llamados criptoángeles) sobre la marcha. Pero es mucho mejor simplemente preguntarle a aquellos que saben si pueden ayudarle.

Mantenga grupos tan pequeños como le sea posible. La experiencia demuestra que la mejor relación entre instructor-aprendiz es de 1.5 o menos.

---

Una CryptoParty es exitosa si la atmósfera es correcta. No importa cuanta gente asista. Sea paciente cuando intente establecer una CryptoParty en su ciudad o comunidad. Difundirla toma tiempo.



# 7

## Orador

Un orador tiene la tarea de abrir la CryptoParty antes de que la gente se dirija a las mesas de su elección. Debe dar un discurso calmo, referido a “que es la CryptoParty y cuales son sus temas” o uno más intenso acerca de “su privacidad, su libertad, cifrar ahora y hacer que los bastardos que impulsan la vigilancia masiva sufran”. Cada orador tiene su propio estilo.

Para más detalles, consulte la sección //Discurso de apertura// más arriba.

### Criptoángeles

Como criptoángel, su tarea es explicar la criptografía a nivel conceptual, de que lo protege (y de que no) y ayudar con la instalación y usar el software relacionado.

Siempre explíquelo a las personas de su grupo con menor nivel de conocimiento, esté atento a las caras de sorpresa y pregunte si todos comprendieron lo que dijo. Aliente la participación y responda las preguntas cada vez que surjan. Cuando alguien dice saber la respuesta deje que la responda.

El aprendizaje debe ser práctico. Nunca toque la computadora de un participante a menos que note que la persona está atascada en algo, y siempre pida permiso para hacerlo. La mayoría de las personas aprenden visualmente, por eso haga pequeños bocetos o diagramas para ayudarlos un poco y puedan entender los conceptos abstractos detrás del software. Si no conoce la respuesta a una pregunta, transmítala a otros participantes o a los criptoángeles, o intente encontrarla con su grupo.

La idea es que la gente sepa como usar las herramientas que aprendan a un nivel básico cuando se vayan de la CryptoParty. Aún mejor, que puedan contarles a sus amigos que ellos ahora usan la “herramienta xyz” y de este modo lograr que comprendan que no fue tan difícil aprenderlas (y que se lo puedan decir a sus amigos, también).

Si necesita más criptoángeles, encuéntrelos en:

- una CryptoParty
- un hacklab
- una universidad
- o entre sus amigos

## Meta-ángelos

Cuando mayor o más caótica sea una CryptoParty en general, lo mejor es tener un meta-ángel, una persona cuya única tarea es asegurarse que todos tengan la mejor experiencia de aprendizaje y que nadie quede afuera.

Como meta-ángel usted no tendrá un tema ni una mesa. En su lugar, tendrá un resumen de los ángeles disponibles, cuáles son sus fortalezas y qué mesa está cubriendo cada tema.

También debe ayudar a quienes arriben tardíamente a encontrar una mesa.

---

Debe facilitar la comunicación entre las mesas. suma que existen preguntas en cada mesa que su ángel no podrá responder. Ayude hallando alguien que sí pueda hacerlo.

Si alguien parece perdido ayúdlo a encontrar la mesa correcta.

Si alguien está indeciso acerca de qué aprender, charle con él para ayudarlo a entender qué le gustaría saber y elijan una mesa.

## **Construcción de una comunidad**

Cosas que puede hacer para que crezca la comunidad local y global de la CryptoParty.

### **Encuentros nocturnos regulares**

Para construir un movimiento sustentable, debe establecer lazos sociales. Un encuentro nocturno habitual de criptoángeles, organizadores, etc. puede servir para este propósito. Diviértase y pase el rato con amigos.

### **Sesiones de entrenamiento**

Los ángeles necesitan una oportunidad para aprender cosas ellos mismos. En una CryptoParty no hay tiempo para ello. Por eso, puede ser una buena idea organizar una sesión de “entrenamiento para entrenadores”.

## Conferencias

Se ha producido una asamblea de CryptoParty en el CCC desde que el movimiento inició. Esto ayudó a conectarnos mundialmente y para intercambiar experiencias.

Aplicar el concepto a más conferencias puede ayudar a la difusión. Y por supuesto, será muy divertido encontrarse con personas de otras ideas. O quizás alguien ya tenga la misma idea y querrá unírseles.

## Recursos

Lenguaje	Enlace	Descripción
inglés	<a href="https://www.level-up.cc/">https://www.level-up.cc/</a>	recurso para la comunidad de entretenimiento acerca de cuidados digitales globales
inglés	<a href="https://www.cryptoparty.in/learn/#links#handbook">https://www.cryptoparty.in/learn/#links#handbook</a>	enlaces a varios manuales

---

Lenguaje	Enlace	Descripción
alemán	https://wiki.piratenpartei.de/HowTo_Partido_Cryptoparty_aleman	como hacer una cryp-toparty según el HowTo_ Partido Cryptoparty Pirata alemán
alemán	https://www.ak-vorrat.org/wiki/cryptoparty_aleman_AK_Verrat	como hacer una cryp-toparty por el grupo activista cryptoparty alemán AK Verrat
español	https://wiki.partidopirata.com.ar/Aprender_Tutoriales,_videos_y_materiales_del_Partido_Pirata_de_Argentina	partidopirata.com. Aprender Tutoriales, videos y materiales del Partido Pirata de Argentina

---



# 8

## Introducción a la versión en español

La siguiente es la versión en español del CryptoParty Handbook realizada por el Partido Pirata de Argentina. Antes de que siga leyendo, creemos necesario hacer algunas aclaraciones.

Hemos respetado fielmente el original traduciendo lo más literalmente posible al texto, algunas veces lo hemos logrado, otras no tanto. Por ejemplo, *click* puede traducirse por hacer click, hacer clic, cliquear, presionar o pulsar. La redundancia típica de estas palabras muchas veces en el mismo párrafo, incluso en la misma oración, hace que la traducción de la misma no sea uniforme. Por cuestión de estilo, la repetición de palabras en la misma oración no es muy agradable en castellano.

A determinadas palabras las hemos traducido por respeto al idioma y a sus expresiones locales. Aunque *email* es de amplio uso en Argentina, preferimos usar correo electrónico, ya que desconocemos la aceptación del original en inglés en la totalidad de las comunidades hispanohablantes.

IMPORTANTE: el manual está inmerso en una profunda cul-

tura open source. En el apéndice podrá ver un artículo llamado “La necesidad del open source”. Prácticamente no hay mención a la importancia del software libre. Disentimos con esta postura. Sin embargo, por respeto al original, dejamos el artículo. Pero añadimos otro, que expresa “Por qué se debería usar software libre y no open source”.

Hemos cambiado “Linux” por una expresión más adecuada, “GNU/Linux”. Para una explicación, consulte el artículo ¿Qué hay en un nombre?.

Ubuntu no es software completamente libre. No lo recomendamos, al igual que tampoco recomendamos Windows ni Mac OS. Un distribución GNU/Linux derivada de Ubuntu pero completamente libre es Trisquel. Para obtener una lista completa, consulte la guía de distribuciones GNU/Linux 100% libres.

¿Por qué no usar Ubuntu? Muy sencillo. Ubuntu provee repositorios específicos de software que no es libre, y Canonical promueve y recomienda explícitamente, bajo el nombre de Ubuntu, software que no es libre en algunos de sus canales de distribución. También ofrece la opción de instalar aplicaciones que no son libres. Además, la versión del kernel Linux que incluye contiene objetos binarios de firmware (blobs). Las políticas de marca registrada de Ubuntu prohíben la redistribución comercial de copias exactas, negando una importante libertad. Además, desde el mes de octubre de 2012, Ubuntu transmite datos personales acerca de las búsquedas realizadas por el usuario a un servidor de Canonical que restituye avisos publicitarios para comprar en Amazon. En sentido estricto, esto no influye en el hecho de si Ubuntu es o no es software libre, sino que se trata de una violación de la privacidad de los usuarios. Además, anima a comprar en Amazon, una empresa involucrada en la DRM (Digital Restrictions Management, Gestión digital de restricciones) como así también en el maltrato de los trabajadores, autores y editores. La inclusión de

---

esta publicidad involuntaria (adware) es uno de los raros casos en que un programador de software libre persiste en conservar una funcionalidad maligna en su versión de un programa.

Bueno, usted decide. Nuestro consejo es que use software libre, no open source (y menos software privativo). A partir de aquí, la traducción completa del texto original en inglés.



# 9

## Consejos básicos

Al igual que con otras formas de comunicación en la web, siempre se deben tomar algunas precauciones básicas para poder proteger nuestra privacidad de manera efectiva.

### Brevemente:

- Las contraseñas no deben estar relacionadas con detalles personales y deben contener una combinación de 8 o más letras y otros caracteres.
- Verifique siempre que su conexión es segura cuando lee correos electrónicos o cuando navega en redes inalámbricas, especialmente en sitios con acceso público a internet.
- Los archivos temporarios (el “caché”) de la computadora que usted usa para revisar sus correos electrónicos pueden presentar riesgos. Bórrelos periódicamente.
- Cree y mantenga cuentas de correo electrónico separadas para distintas tareas e intereses.
- Cifre todos los mensajes que no se atrevería a escribir en una tarjeta postal.

- Sea precavido con los riesgos que implica que su correo electrónico esté hospedado en una empresa u organización.

## Contraseñas

Las contraseñas son el punto más vulnerable en la comunicación de correos electrónicos. Incluso una contraseña segura puede ser interceptada a menos que la conexión sea segura (consulte TLS/SSL en el glosario). Además, que una contraseña sea larga no significa que no pueda ser adivinada usando conocimientos de su persona y de su vida privada.

La regla general para crear contraseñas es que deben ser largas (8 caracteres o más) y tener una mezcla de letras y otros caracteres (números y símbolos, lo que significa que usted no debe elegir una oración breve). Combinar la fecha de su cumpleaños con un nombre familiar es un gran ejemplo de lo que no debe hacerse. Este tipo de información es fácil de encontrar usando recursos públicos. Un truco popular es basarse en una frase favorita y entonces, sólo para confundir, se mezcla con algunos números. Lo mejor de todo es el uso de un generador de contraseñas, ya sea en el sistema local o en forma online.

A menudo, las contraseñas son difíciles de recordar y por eso aparece un segundo punto de vulnerabilidad - el descubrimiento de su registro escrito. Puesto que no hay mejor medio de almacenar una contraseña que en su propio cerebro, servicios como OnlinePasswordGenerator(<http://www.onlinepasswordgenerator.com/>) ofrecen un gran compromiso por generar contraseñas al azar que recuerdan vagamente a las palabras y les presentará una lista para elegir.

Si usted no elige memorizar sus contraseñas, deberá escribirlas o usar un software de cadena de claves. Esto puede ser una decisión riesgosa, especialmente si la cuenta de correo electrónico

---

y la contraseña son las mismas para dispositivos diferentes tales como su teléfono o su computadora.

El software de cadena de claves, tal como KeePass, reúne varias contraseñas y frases de paso en un lugar y posibilita su acceso a través de una contraseña o frase de paso maestra. Esto le pone presión a la elección de esta clave maestra. Si decide usar un software de cadena de claves, recuerde elegir contraseñas seguras.

Por último, debe usar una contraseña diferente para cada cuenta. De esta manera, si una de ellas es robada, las otras cuentas permanecerán seguras. Nunca use la misma contraseña para las cuentas de correo electrónico laborales y para las personales. Vea la sección **Contraseñas** para aprender más acerca de cómo protegerse.

## Leyendo correos electrónicos en lugares públicos

Uno de las principales ventajas de las redes inalámbricas y la “computación en la nube” es la posibilidad de trabajar en cualquier lugar. A menudo, puede revisar su correo en un café con conexión a internet o en algún otro lugar público. Los espías, criminales y todo tipo de malvivientes a menudo frecuentan estos lugares para aprovechar las grandes oportunidades que ofrecen para el robo de identidad, el espionaje electrónico y el saqueo de cuentas bancarias.

Aquí nos encontramos a menudo con un riesgo a menudo subestimado de que alguien escuche nuestras comunicaciones usando un *paquete de sniffing de redes*. No es tan importante que la red sea abierta o está asegurada por una contraseña. Si alguien se une a la misma red cifrada, puede capturar y leer fácilmente

todo el tráfico inseguro (vea el capítulo **Conexión segura**) de todos los otros usuarios que están dentro de la misma red. Una clave de acceso inalámbrica se puede adquirir por el precio de una taza de café y les da -a las personas con conocimientos de lectura y captura de paquetes en la red- la oportunidad de leer su contraseña mientras revisa sus correos electrónicos.

Aquí tiene una sencilla regla que siempre debe cumplir: si el café ofrece una conexión cableada, júsela! Además, asegúrese de que nadie está viendo sobre su hombro cuando tipee su contraseña.

## Almacenamiento malicioso

Una vez más la conveniencia rápidamente nos lleva por mal camino. Debido a la molestia general de tener que escribir las contraseñas una y otra vez, las almacenamos en el navegador o cliente local de correo electrónico. Esto no es malo en sí mismo, pero cuando nos roban la computadora o el teléfono móvil, el ladrón puede acceder a nuestra cuenta de correo electrónico. Lo más recomendable es limpiar la memoria caché siempre que cierre su navegador. Todos los navegadores populares tienen una opción para borrar la memoria caché al salir.

Si aún así decides almacenar en memoria tus contraseñas, deberías cifrar tu disco. Si tu computadora es robada y el ladrón reinicia la máquina, va a encontrarse con un disco cifrado. También es aconsejable tener un bloqueo de pantalla instalado. Si le roban la máquina mientras navega, no podrán acceder a ella.

## Asegurando su comunicación

Mientras escriba y envíe correos electrónicos mediante un navegador o un programa (Outlook Express, Mozilla Thunderbird,

---

Mail.app o Mutt), asegúrese de que la sesión completa esté cifrada. Esto es fácil de hacer debido al uso de conexiones *TLS/SSL (Secure Socket Layer)* en los servidores de correo electrónico (Consulte en el glosario **TLS/SSL**).

Si usa un navegador para revisar su correo, verifique que su servidor soporta sesiones SSL comprobando que la URL comienza con `https://`. Si este no es el caso, asegúrese de activarlo en la configuración de cuentas de correo electrónico, tales como Gmail o Hotmail. Esto asegura que no sólo la parte de la sesión de inicio de sesión de correo electrónico está cifrado, sino también la escritura y el envío de correos electrónicos. Además verifique los detalles del certificado, tenga en cuenta el *TLS pinning* y respalde las extensiones del navegador web que advierten acerca de los cambios o los certificados disfuncionales (por ejemplo, *Certificate Patrol*) y haga uso de la versión segura TLS del sitio web como default (por ejemplo *HTTPS everywhere*).

El proveedor de servicios de correo electrónico que usted elija debería brindarle a usted detalles de su servidor de correos. Estos detalles pueden hallarse a menudo en la sección de configuración. Si su servicio de correo electrónico no proporciona TLS/SSL para cifrar sus datos, entonces le aconsejamos que deje de usarlo. Incluso si sus mensajes no son importantes, puede que un día se encuentre “inhabilitado” para acceder a su cuenta ¡porque su contraseña ha sido cambiada!

Cuando use un programa de correo electrónico para ver sus mensajes, asegúrese de usar la opción TLS/SSL. Por ejemplo, en Mozilla Thunderbird la opción para asegurar su correo saliente se encuentra en `Edit -> Account Settings -> Outgoing Server (SMTP)`, para correo entrante está en `Edit -> Account Settings -> Server Settings`. Esto nos asegura que la descarga y envío de mensajes esté cifrada, dificultando su lectura o la de sus registros para cualquier persona de su propia red o que se encuentre entre usted y su servidor de correo elec-

trónico. Además, cifre el mensaje en sí mismo. Nota del traductor: cuando ejemplifiquemos con Thunderbird, usaremos la última versión al momento de escribir esta traducción, febrero del 2013, que difiere sensiblemente de las anteriores. Por ejemplo, las configuraciones mencionadas más arriba, en las versiones de Thunderbird anteriores se encuentran en Tools y no en Edit. Asimismo, la barra de menú no aparece visible por defecto en la versión actual, para verla debe hacer un click con el botón derecho del ratón en la barra donde se encuentra la solapa **Inbox** y tildar la opción **Menu bar**.

Aunque la línea esté cifrada usando un sistema como SSL, el proveedor de correo electrónico aún tiene acceso a los mensajes porque tiene un acceso completo al dispositivo de almacenamiento de su correo electrónico. Si desea usar su servicio web asegúrese que su proveedor no pueda leer sus mensajes, para eso necesitará algo conocido como *GPG* (en el apéndice, **GnuPG**) con el cual podrá cifrar su mensaje. El encabezado de su mensaje, sin embargo, aún contiene la IP (Internet address, dirección IP) a partir de la cual se envió y otros detalles comprometedores. Vale la pena mencionar que usar *GPG* en webmail no es tan sencillo como en los clientes localmente instalados, tales como *Thunderbird* o *Outlook Express*.

## DNSSEC & DANE

La información del certificado puede estar almacenada en registros DNS y sin embargo ser más fiable y segura. Verifique la disponibilidad de *DNSSEC* y especialmente considere los servicios de correo electrónico *DANE* con su proveedor de servicios. En este punto, nuevamente las extensiones del navegador web (por ejemplo *DNSSEC/TLSA Validator*) pueden ayudarlo para controlar la disponibilidad de estas medidas de seguridad.

---

## **Separación de cuentas**

Debido a la conveniencia de servicios como Gmail, es cada vez más común que las personas usen una única cuenta de correo electrónico. Esto aumenta considerablemente el daño potencial que provocaría si tuviéramos algún problema con ella. Más aún, nada impide que algún empleado disgustado de Google borre o robe su cuenta, sin olvidar que el propio Google puede ser hackeado. Estas cosas suceden.

Una estrategia práctica es mantener su cuenta personal de esa manera. personal. Si dispone del servicio de correo electrónico en su trabajo, cree una cuenta nueva si su empleador aún no lo ha hecho por usted. Lo mismo para todo club u organización a la cual pertenezca, con contraseñas diferentes. No sólo mejora su seguridad, sino que también reduce el riesgo de un robo completo de identidad y disminuye enormemente la cantidad de spam.

## **Nota acerca del almacenamiento de correos electrónicos**

Los proveedores de servicios de almacenamiento, envío, descarga y lectura de correos electrónicos no se destacan precisamente por el uso de TLS/SSL. Al almacenarlos, pueden leer y registrar sus mensajes en texto plano. Pueden cumplir con los pedidos de las agencias de seguridad locales que deseen acceder a su cuenta. También pueden analizar sus mensajes para obtener patrones, palabras claves o signos de sus afinidades con determinados grupos políticos, ideologías o marcas comerciales. Por eso es muy importante leer el contrato de licencia de uso del usuario final de su proveedor de correo electrónico y realizar una pequeña investigación acerca de sus afinidades e intereses antes de ele-

girlo. Todo lo referido anteriormente también se aplica a los destinatarios de sus mensajes.

# 10

## Tipos de correo electrónico

El correo electrónico se puede usar de dos maneras:

- Lectura, escritura y envío de mensajes desde un *navegador web* (webmail), o
- Lectura, escritura y envío usando un *programa de correo electrónico*, como Mozilla Thunderbird, Mail.App o Outlook Express utilizando protocolos tales como *SMTP*, *POP* e *IMAP*.

Estos dos modelos pueden ser mixtos en la práctica, especialmente si se usa *IMAP*. Aunque el webmail es la solución más adecuada para usar y más fácil de mantener para usuarios finales que usen diferentes computadoras comparada con las soluciones más poderosas (más almacenamiento, mejores opciones de búsqueda y control directo de los datos) basadas en las aplicaciones nativas

## Correo electrónico almacenado remotamente (“webmail”) usando un navegador web

Los mensajes enviados por medio del *browser*, a veces llamado *webmail*, consisten en una cuenta con un almacenamiento remoto de correo electrónico tal como Google (Gmail), Microsoft (Hotmail) o Yahoo (Yahoo Mail). Las oportunidades de negocios abiertas al almacenar mensajes de correo de otras personas son muchas: contacto con otros servicios ofrecidos por la empresa, exposición de marcas comerciales y lo más importante, búsqueda entre sus mensajes de patrones que puedan ser usados para evaluar sus intereses – algo de gran valor en la industria de la publicidad (aunque también para determinados gobiernos). Por razones de data mining, dichas compañías *no están interesadas* en alentar a sus usuarios para que usen *cifrado para asegurar la privacidad y/o firmas para la integridad/autenticidad* de la comunicación.

## Correo electrónico almacenado remotamente usando un programa o un navegador web

Un programa de correo electrónico tal como Outlook, Thunderbird o Mail.App también puede ser usado con un servicio de webmail como Gmail o su compañía proveedora de servicio de correo electrónico. En cualquier caso, los mensajes aún pueden ser descargados en su computadora pero están retenidos en su servidor de correo (por ejemplo Gmail). De esta manera, para acceder a los mensajes no se requiere del uso del navegador todo el tiempo, pero aún estará usando Gmail, Hotmail, etc. como

---

servicio. La diferencia entre almacenar los mensajes en su computadora con un programa de correo y hacerlo remotamente en un servidor (por ejemplo Hotmail, Gmail o el servidor de su universidad) en Internet puede parecer algo confuso al principio.

Finalmente, también se pueden enviar mensajes a un servidor de correo electrónico sin que se almacenen allí en absoluto, simplemente lo reenvía a su destino tan pronto como llega al servidor de reenvío de correo electrónico. Google y Microsoft no permiten este tipo de configuración. Más bien esto suele ser algo que su universidad o empresa proveerá para usted. Tenga en cuenta que esto conlleva el riesgo de que el administrador del sistema haga copias secretamente de sus mensajes a medida que entran y salen del servidor.

En general, el uso de webmail combinado con la descarga de los mensajes usando un programa de correo electrónico es la mejor opción. Este enfoque añade redundancia (copias de seguridad locales) junto a la opción de borrar todo el correo electrónico desde el servidor remoto una vez descargado. Esta última opción es ideal para la información de contenido sensible donde la posibilidad de robo de cuentas es alto, pero corre el riesgo de pérdida total de los mensajes si la máquina local falla y no se dispone de copias de seguridad. En segundo lugar, cuando se utiliza un programa de correo electrónico, tenemos la opción de cifrar los mensajes, como el popular GPG, algo que no es fácil de configurar y utilizar en servicios de correo web con uso exclusivo del navegador. En cualquier caso, el cifrado del disco rígido en el equipo local es altamente recomendable (consulte el Apéndice **Cifrado de disco**).

## Consideraciones de contexto

Usted puede administrar un servidor y correr su propio servicio de correo electrónico. O almacenar sus mensajes en su empresa o en el servidor de sus jefes. Finalmente, usted puede usar un servicio mediante una corporación, por ejemplo Google (Gmail) or Microsoft (Hotmail). Cada uno presenta una interesante combo de consideraciones que se refieren precisamente al hecho básico de que a menos que la propia dirección de correo electrónico está cifrada, el administrador del servidor de correo electrónico aún puede copiar secretamente el correo electrónico en el momento que llegue al servidor. No importa que usted esté utilizando *TLS/SSL* (consulte el Apéndice **SSL**) para ingresar y consultar su correo electrónico, ya que sólo protege la conexión entre el equipo local y el servidor.

Como siempre, si conoce los riesgos y se siente preocupado es sabio escuchar estos consejos - no envíe correos electrónicos sensibles utilizando un servicio que no sean de confianza.

## Empleador/Organización

Su empleador o la organización que esté involucrada está en excelente posición para aprovecharse de su confianza y leer los mensajes de su cuenta de correo electrónico laboral que se almacenan en el servidor, tal vez en un esfuerzo por aprender acerca de usted, de sus motivaciones, agendas e intereses. Estos casos de espionaje del empleador hacia el empleado son tan comunes que no merecen atención. La única solución es el cifrado del correo electrónico usando, por ejemplo, GPG (consulte el Apéndice **GPG**).

---

## Correos electrónicos & metadata

La información del contenido actual de los correos puede ser preservada usando *OpenPGP* o *S/MIME* pero los metadatos - la asociación de personas, direcciones, tiempo y software y/o servicios usados - son almacenados por diversas plataformas. Los servicios gubernamentales pueden almacenar datos así como también las compañías involucradas en transmitirlos. Con respecto a la información del encabezado del mensaje de correo, permanece en riesgo durante la comunicación así como también las cuentas usadas pueden ser conectadas con individuos o grupos

## Servidor de correo auto administrado

Esta es la configuración ideal de almacenamiento, pero requiere un alto grado de conocimientos técnicos. Aquí, en general, los riesgos a la privacidad no son sólo proteger su propia cuenta contra intentos de exploits (contraseñas débiles, sin SSL) sino que conlleva una gran responsabilidad, y tal vez sucumba a la tentación de leer los correos electrónicos de aquellas personas a las cuales les presta servicio.

## Servicios de correo electrónico “gratuitos”

Como se mencionó anteriormente los riesgos de almacenar y enviar mensajes con un servicio prestado por una empresa son bastante altos si valora su derecho ciudadano a la privacidad. Las empresas que almacenan sus cartas de amor, sus expresiones y

sus diarios corren el riesgo de ceder a las presiones de los intereses de orden político, económico y de las fuerzas de seguridad del país al que están legalmente sujetas. Un usuario de Gmail Malasia, por ejemplo, corre el riesgo de exponer sus intereses y sus propósitos a un gobierno que no eligieron, por no hablar de los socios comerciales de Google interesados en ampliar su alcance en el mercado.

## **Sin fines de lucro**

Distintos servidores web ofrecen cuentas de correo electrónico gratuitas a las organizaciones sin ánimo de lucro o filantrópicos como ellos. Algunos incluso ofrecen wikis, listas de correo, chats y redes sociales. Una consideración para las organizaciones que trabajan en el campo político: puede haber diferencias de intereses entre el estado en el que se aloja el correo electrónico y los intereses políticos de la organización por medio de ese servicio. Tales riesgos idealmente se deben reflejar en el Acuerdo de Licencia de Usuario Final.

## **Notas sobre reenvío de correo electrónico**

Los servicios de reenvío de mensajes proporcionan la ventaja de “enlazar” una cuenta con otra de la forma que el usuario crea conveniente. Esto por supuesto es más comúnmente utilizado cuando el titular de la cuenta está de vacaciones y quiere que sus mensajes sean derivados desde su cuenta de trabajo a otra que utilizará durante el viaje o que está inaccesible fuera del lugar de trabajo. El riesgo con cualquier servicio de reenvío de correo electrónico externo es el mismo que el riesgo de alojarlo

---

de forma remota en servicios como Gmail, por ejemplo: puede ser copiado y almacenado. Aquí, el cifrado usando un sistema como *GPG* (consulte el Apéndice **GPG**) le asegurará de que si se copia por lo menos no se podrá leer.



# 11

## Temores

*¿Quién puede leer los mensajes de correo electrónico que he enviado o recibido?*

*¿Quién puede leer los correos electrónicos que envío cuando viajan a través de Internet?*

*¿Las personas que reciben mis mensajes pueden compartirlos con alguien?*

Los correos electrónicos que se envían “en texto plano”, sin ningún tipo de cifrado (la gran mayoría de los correos electrónicos enviados y recibidos en la actualidad) se pueden leer, registrar, e indexar por medio de cualquier servidor o router a lo largo del camino, mientras el mensaje viaja del emisor al receptor. Suponiendo que utiliza una conexión cifrada (ver el glosario para TLS/SSL) entre sus dispositivos y su proveedor de servicios de correo electrónico (lo que todo el mundo debería hacer), esto significa en la práctica que las siguientes personas todavía pueden leer cualquier mensaje enviado:

1. Usted
2. Su proveedor de correo electrónico

3. Los operadores y los dueños de cualquier conexión intermedia de red (a menudo conglomerados multinacionales o incluso estados soberanos)
4. El proveedor de servicio de correo electrónico del destinatario
5. El destinatario previsto

Muchos proveedores de correo web (como Gmail) automáticamente inspeccionan todos los mensajes enviados y recibidos por sus usuarios con el fin de mostrar anuncios dirigidos. Si bien esto puede ser un compromiso razonable para algunos usuarios (¡libertad al correo electrónico!), la mayoría de las veces es preocupante para muchas personas ya que incluso sus comunicaciones más íntimas son inspeccionados y catalogadas como parte de un perfil mantenido oculto y potencialmente muy interesante para cualquier poderoso gigante corporativo con fines de lucro.

Además, alguien que legalmente puede presionar a los grupos anteriormente mencionados podría solicitar o exigir:

1. metadatos registrados sobre los mensajes (listas de mensajes enviados o recibidos por cualquier usuario, asunto de los mensajes, destinatarios), injustificada en algunas jurisdicciones.
2. mensajes enviados y recibidos por un grupo específico de usuarios o grupos, con justificación u orden judicial en algunas jurisdicciones.
3. una conexión dedicada a desviar *todos* los mensajes y *todo* el tránsito, para ser analizados e indexados fuera del sitio.

En los casos donde un usuario tiene una relación comercial o de servicio con su proveedor de correo electrónico, la mayoría de los gobiernos van a defender los derechos de privacidad del usuario contra la lectura no autorizada e injustificada o el intercambio de mensajes, aunque a menudo es el propio gobierno quien busca información, y con frecuencia los usuarios renuncian

---

a algunos de estos derechos como parte de su acuerdo de servicio. Sin embargo, cuando el proveedor de correo electrónico es el empleador del usuario o institución académica, los derechos de privacidad con frecuencia no se aplican. Dependiendo de la jurisdicción, las empresas en general tienen el derecho legal a leer todos los mensajes enviados y recibidos por sus empleados, incluso los mensajes personales enviados después de hora o en las vacaciones.

Históricamente, era posible “eludirlos” con el uso de correo electrónico en texto plano, porque el costo y el esfuerzo de almacenar e indexar el creciente volumen de los mensajes era demasiado alto: alcanzaba para que los mensajes fueran entregados confiablemente. Por ello, muchos sistemas de correo electrónico no contienen mecanismos para preservar la privacidad de sus contenidos. Ahora bien, el costo de la vigilancia ha bajado mucho más rápidamente que el crecimiento del tráfico de Internet y es razonable esperar la vigilancia a gran escala y la indexación de todos los mensajes (ya sea en el remitente o del lado del receptor) aún para usuarios y los mensajes más inocuos. [CITA: espionaje/archivado de correo electrónico corporativo, bluecoats, el seguimiento de Siria, centro de datos en Utah, EEUU, los escándalos de intercepción en EEUU]

Para más información sobre la protección legal de los mensajes de correo electrónico “en reposo” (término técnico para los mensajes almacenados en el servidor después de haber sido enviados), en especial con respecto a los accesos del gobierno a estos mensajes de correo, vea:

- <https://ssd.eff.org/3rdparties/govt/stronger-protection> (USA)
- [http://en.wikipedia.org/wiki/Data\\_Protection\\_Directive](http://en.wikipedia.org/wiki/Data_Protection_Directive) (EU)

Así como hay ciertas fotos, cartas, y credenciales que usted no sube “en texto plano” en Internet porque no quiere que esa in-

formación sea indexada accidentalmente y se muestre en los resultados de búsqueda, nunca se deben enviar mensajes de correo electrónico “en texto plano” si no quiere que un empleador o un oficial de seguridad del aeropuerto disgustado tenga fácil acceso al mensaje.

## **Abusos al azar y robo por parte de hackers maliciosos**

*¿Qué pasa si alguien toma el control completo de mi cuenta de correo electrónico?*

*Me he conectado desde un lugar inseguro ... ¿cómo puedo saber ahora si mi cuenta ha sido hackeada?*

*No he hecho nada malo... ¿qué tengo que esconder?*

*¿Por qué alguien se preocupa por mí?*

Por desgracia, hay muchos incentivos prácticos, sociales y económicos para que los hackers maliciosos irrumpan en las cuentas de individuos al azar de Internet. El incentivo más evidente es el robo de identidad y financiero, cuando el atacante puede estar tratando de obtener acceso a los números de tarjetas de crédito, credenciales de compras del sitio, o información bancaria para robar dinero. Un hacker malicioso no tiene manera de saber de antemano que usuarios son mejores blancos que otros, por lo que sólo tratan de irrumpir en todas las cuentas, incluso si el usuario no tiene nada para robar o toma recaudos para no exponer su información.

Menos evidentes son los ataques para obtener acceso a las cuentas de usuario válidas y confiables para recolectar direcciones de correo electrónico de contactos y luego distribuir spam en forma masiva, o para acceder a determinados servicios vinculados a

---

una cuenta de correo electrónico, o para usarla como un “trampolín” en sofisticados ataques de ingeniería social. Por ejemplo, una vez controlada la cuenta un hacker malicioso podría rápidamente enviar correos electrónicos a sus socios o compañeros de trabajo solicitando un acceso de emergencia a los sistemas informáticos más seguros.

Un último problema inesperado que afecta incluso a los usuarios de bajo perfil de correo electrónico, es el secuestro masivo de cuentas en grandes proveedores de servicios, cuando los hackers maliciosos acceden a la propia infraestructura de hosting y extraen contraseñas e información privada en grandes cantidades, y luego vender o publicar listas de información de inicio de sesión en mercados online.

## Abuso dirigido, acoso y espionaje

*Algo que escribí enfureció a una persona en el poder... ¿Cómo puedo protegerme?*

Si usted es un objetivo individual de atención por parte de poderosas organizaciones, gobiernos o individuos determinados, entonces deberá aplicar las mismas técnicas y principios para mantener la seguridad y la privacidad de su correo electrónico, pero deberá tomar medidas adicionales para protegerse de hackers maliciosos que utilizan técnicas sofisticadas para socavar sus dispositivos y cuentas. Si un hacker malicioso toma el control de alguno de sus dispositivos de computación o tiene acceso a cualquiera de sus cuentas de correo electrónico, es probable que pueda acceder en forma inmediata tanto a la totalidad de su correspondencia, como a cualquiera de los servicios externos vinculados a su cuenta de correo electrónico.

Los esfuerzos para protegerse contra este tipo de ataques pueden sufrir una gran escalada hasta extenderse rápidamente en una

batalla de voluntades y recursos, pero algunas pautas básicas pueden ayudarlo. Use dispositivos exclusivos para las comunicaciones. Desconecte y apague los dispositivos inmediatamente después de que haya terminado de usarlos. Lo mejor es utilizar herramientas de cifrado, navegadores web y sistemas operativos de software libre ya que pueden sus problemas de seguridad pueden ser revisados públicamente y solucionados con los parches de seguridad.

*Ten cuidado al abrir archivos PDF con Adobe Reader u otros lectores de PDF propietarios.* Los lectores de PDF de código cerrado han sido utilizadas para ejecutar código maligno incorporado en el cuerpo del PDF. Si recibe un pdf como archivo adjunto primero debe considerar si se conoce el presunto emisor y si usted está esperando un documento de él. En segundo lugar, puede utilizar lectores de PDF que han sido probados en busca de vulnerabilidades conocidas y no ejecutar código a través de javascript.

GNU/Linux: Evince, Sumatra PDF

OS X: Preview

Windows: Evince

Use contraseñas generadas al azar siempre que sea posible.

## Cuando el cifrado funciona mal

*¿Qué pasa si pierdo mis “claves”? ¿Pierdo mi correo electrónico?*

Estrictamente hablando, el cifrado GPG de correo electrónico no deja de tener sus propios problemas.

Si almacena su correo electrónico cifrado y pierde todas las copias de su clave privada, será absolutamente incapaz de leer

---

los mensajes antiguos almacenados, y si usted no tiene una copia de su certificado de revocación para la clave privada sería muy difícil probar que cualquier nueva clave que genere es válida, al menos hasta que la clave privada original expire.

Si usted firma un mensaje con su clave privada, tendrá grandes dificultades para convencer a alguien de que no lo hizo si el destinatario revela el mensaje y la firma públicamente. El término para esto es *sin repudio*: cualquier mensaje que envíe firmado es una excelente evidencia en una corte. Además, si la clave privada es robada, podría ser utilizada para leer todos los mensajes cifrados enviados a usted alguna vez con su clave pública: los mensajes pueden estar seguros cuando se encuentran en tránsito y en el momento en que se reciben, pero las copias son una responsabilidad y dependen de que la clave privada nunca sea revelada. En particular, incluso si se destruye cada mensaje justo después de leerlo, cualquiera pueda interceptar el mensaje en el hilo, guardar una copia y tratar de descifrarlo más tarde si obtiene la clave privada.

La solución es utilizar un protocolo de mensajería que proporciona un *secreto-perfecto-haciaadelante* mediante la generación de forma aleatoria de una nueva clave de sesión única para cada conversación de intercambio de mensajes de tal manera que no puedan ser generadas a posteriori, aunque sean conocidas las claves privadas. El protocolo de chat ([https://es.wikipedia.org/wiki/Perfect\\_forward\\_secrecy](https://es.wikipedia.org/wiki/Perfect_forward_secrecy)) lo garantiza en el caso de la mensajería instantánea en tiempo real, y el protocolo SSH lo proporciona para las conexiones de shell remoto, pero no existe un sistema equivalente para el correo electrónico en este momento.

Puede ser difícil de sopesar la comodidad del acceso móvil a sus claves privadas con el hecho de que los dispositivos móviles son mucho más fáciles de perder, ser robados o hackeados que las máquinas fijas. Cualquier urgencia podría ser el momento

exacto en que usted más desea enviar un mensaje confidencial o un mensaje firmado para verificar su identidad, pero también es el momento en el puede que no tenga acceso a las claves privadas si su dispositivo móvil está intervenido o no está cargado con todas sus claves.

# 12

## Conexiones seguras

**¿Otras personas pueden leer mis mensajes mientras verifico mi correo electrónico?**

Como vimos en el Capítulo **Basic Tips**, aunque utilice correo web o un programa de correo electrónico usted siempre debe asegurarse de utilizar el cifrado para la sesión entera, desde el inicio hasta cerrar la sesión. Esto evitará que cualquier persona espíe su comunicación con su proveedor de correo electrónico. Afortunadamente, esto es fácil de hacer debido al uso popular de las conexiones *TLS/SSL* en los servidores de correo electrónico (ver apéndice **TLS/SSL**).

Una conexión TLS/SSL en el navegador, cuando se utiliza correo web, aparecerá con `https` en la URL, en lugar de la norma `http`, por ejemplo:

`https://gigglemail.com`

Si su servidor de correo web no ofrece un servicio de TLS/SSL, entonces debería considerar la suspensión del uso de esa cuenta,

aunque sus propios correos electrónicos no son especialmente privados o importantes, su cuenta puede ser fácilmente hackeada descubriendo su contraseña por “sniffing”. Si aún no está activado, asegúrese de hacerlo en las opciones de su cuenta. Al momento de escribir el libro, Gmail de Google y Hotmail/Microsoft Live cambian automáticamente su explorador para utilizar una conexión segura.

Si está utilizando un programa de correo electrónico como Thunderbird, Mail.app o Outlook, asegúrese de comprobar que está utilizando TLS/SSL en las opciones del programa. Consulte el capítulo **Configuración de conexiones seguras** en la sección de **Seguridad del correo electrónico**.

## Notas

Es importante tener en cuenta que los administradores de los proveedores como Hotmail o Google, que albergan, reciben o envían su correo electrónico, pueden leerlo aunque utilice conexiones seguras. También es destacable que las claves criptográficas que protegen una conexión TLS/SSL pueden ser deliberadamente reveladas por los operadores de los sitios web, o copiadas sin su permiso, violando la confidencialidad de su conexión. También es posible que un Certificado de Autorización esté corrupto o comprometido entonces se creará un certificado falso de las claves mantenido por espías, lo que facilita el ataque man in the middle sobre las conexiones que utilizan TLS/SSL (Véase el Glosario para “Ataque Man in the Middle”). A modo de ejemplo, vea el siguiente caso <http://cryptome.info/0001/nsa-ssl-email.htm> que involucra a la NSA de Estados Unidos y a varios proveedores de correo electrónico.

También notemos que el uso de una *Red Privada Virtual* es otra buena manera de asegurar sus conexiones al enviar y leer correo

---

electrónico, pero requiere el uso de un cliente VPN en el equipo local que se conecta a un servidor. Consulte el capítulo **Red Privada Virtual** en la sección de **navegación**.



# 13

## Correo electrónico seguro

Es posible enviar y recibir mensajes seguros utilizando los programas estándares de correo electrónico actuales mediante la adición de unos pocos complementos. La función esencial de estos complementos es hacer que el cuerpo del mensaje (pero no los campos Para:, De:, CC: y Asunto:) sea ilegible para cualquier tercera parte que intercepte o acceda de otro modo a su correo electrónico o a la de su compañero de conversación. Este proceso se conoce como cifrado.

Para asegurar los mensajes se utiliza generalmente una técnica llamada *Criptografía de clave pública*. La criptografía de clave pública es una técnica inteligente que utiliza dos claves de codificación para enviar un mensaje. Cada usuario tiene un *clave pública*, la cual sólo puede ser utilizada para cifrar un mensaje, pero no para descifrarlo. Las claves públicas son bastante seguras para no tener que preocuparse de que alguien pudiera descubrirlos. La *clave privada* es mantenida en secreto por la persona que recibe el mensaje y se puede utilizar para descifrar los mensajes codificados con la clave pública correspondiente.

En la práctica, eso significa que si Rosa quiere enviarle un mensaje seguro a Heinz, sólo necesita su clave pública para codificar

el texto. Al recibir el correo electrónico, Heinz a continuación utiliza su clave privada para descifrar el mensaje. Si quiere responder, tendrá que utilizar la clave pública de Rosa para cifrar la respuesta, y así sucesivamente.

## ¿Qué software puedo usar para cifrar mi correo electrónico?

La configuración más popular para la criptografía de clave pública es el uso de *Gnu Privacy Guard (GPG)* para crear y administrar claves y un complemento para integrarla con el software de correo electrónico estándar. El uso de GPG le dará la opción de cifrar correo electrónico sensible y decodificar el correo entrante que ha sido cifrada pero no estará obligado a usarlo todo el tiempo. Años atrás era muy difícil de instalar y configurar, pero avances recientes han hecho que este proceso sea relativamente simple.

Consulte la sección **Cifrado de correo electrónico** para trabajar con GPG en el ámbito de su sistema operativo y su programa de correo electrónico.

Si utiliza un servicio de *webmail*, es más difícil cifrar el correo electrónico. Puede utilizar un programa GPG en su computadora para cifrar el texto utilizando su clave pública o puede utilizar un complemento, como Lock The Text (<http://lockthetext.sourceforge.net/>). Si desea mantener los mensajes privados, le sugerimos que utilice un programa de correo electrónico dedicado como Thunderbird en lugar de webmail.

# 14

## Consejos básicos

### Brevemente:

- Cuando visite un sitio web no dé ninguna información acerca de usted mismo al dueño del sitio sin tomar algunas precauciones.
- Su navegación en Internet puede ser rastreada por los sitios que visita y por los socios de estos sitios. Use software antiseguimiento.
- La visita a un sitio web nunca es una conexión directa. Muchas computadoras, de distintos dueños, están involucradas. Use una conexión segura para evitar que su sesión web sea registrada.
- Lo que usted busca es lo que más le importa a los proveedores de los buscadores. Use software de búsqueda anónima para proteger su privacidad.
- Es más prudente confiar en los navegadores de código abierto como Mozilla Firefox, ya que su seguridad puede ser auditada más fácilmente.

## **Su navegador habla de usted por detrás suyo**

Todos los navegadores comunican información al servidor web que almacena la página que usted visita. Esta información incluye el nombre y la versión del navegador, la información de referencia (un enlace desde otro sitio, por ejemplo) y el sistema operativo utilizado.

Los sitios web suelen utilizar esta información para personalizar su experiencia de navegación, lo que sugiere descargas para su sistema operativo y formatear la página web para adaptarla mejor a su navegador. Naturalmente, esto presenta un problema en lo que al anonimato del usuario ya que esta información forma parte de un conjunto más amplio de datos que pueden ser utilizados para identificarlo en forma individual.

Detener la charla de su navegador no es fácil de hacer. Usted puede, sin embargo, falsificar alguna parte de la información enviada a los servidores web mientras navega por la alteración de los datos contenidos en el archivo *User Agent*, la identidad del navegador. Hay un plugin muy útil para Firefox, por ejemplo, el llamado *User Agent Switcher* que le permite establecer la identidad del navegador a otro perfil seleccionado de una lista desplegable de opciones.

## **Los sitios web pueden rastrear por dónde usted navega**

A menudo, los sitios web escriben en su computadora pequeños archivos llamados cookies. Estos cookies presentan ciertas ventajas, como almacenar datos de inicio de sesión, información de sesión y otros datos que hacen a su experiencia de navegación

---

más llevadera. Estas pequeñas piezas de información son muy peligrosas para su derecho al anonimato en la web: pueden ser usadas para identificarlo si retorna al sitio y también puede registrar como navega entre diferentes sitios. Junto con el User-Agent, representan un medio poderoso y secreto para identificar remotamente a su persona.

La solución ideal para este problema es denegar todos los intentos del sitio web para escribir cookies en su sistema sin embargo esto puede reducir significativamente la calidad de su experiencia en la web.

Consulte la sección **Seguimiento** para ver guías de cómo impedir el rastreo de sitios web sobre usted.

## Búsqueda online de información acerca de usted mismo

Cuando usamos buscadores tales como Bing o Google ponemos en riesgo nuestro derecho a la privacidad, mucho más que cuando respondemos, por ejemplo, a una persona del sector de Informaciones en un aeropuerto.

La información combinada del uso de datos de User Agent y las cookies pueden usarse para construir un retrato suyo en tiempo real. Los publicistas consideran a esta información muy valiosa, y la usan para hacer hipótesis acerca de sus intereses y del mercado de los productos de una manera más específica.

Mientras que algunos clientes pueden cantar alabanzas de la publicidad dirigida y a otros los tiene sin cuidado, los riesgos son a menudo mal entendidos. En primer lugar, la información recopilada acerca de usted puede ser solicitada por un gobierno, incluso un gobierno que no eligieron (Google, por ejemplo, es una empresa estadounidense y por lo tanto debe cumplir con

los procesos judiciales estadounidenses y sus intereses políticos). En segundo lugar, existe el riesgo que la mera búsqueda de información pueda ser mal interpretada como la intención o el apoyo político. Por ejemplo, el estudio de un artista de la estética de las diferentes formas de extremismo religioso lo pone en peligro de ser asociado con el apoyo de las organizaciones estudiadas. Por último, existe el riesgo de que este perfil oculto pueda ser vendido a los agentes de seguros, a sus posibles empleadores o a los clientes de la empresa cuyo servicio de búsqueda está utilizando.

Incluso aunque se haya asegurado que las cookies se borraron, su *User Agent* ha sido cambiado (vea más abajo y en el capítulo de **Seguimiento**) y todavía está informando un dato crucial: la dirección de Internet de dónde se conecta (vea el capítulo **¿Qué sucede mientras navega**). Para evitar esto, puedes usar un servicio de anonimato como Tor (ver capítulo **Anonimato**). Si usted es un usuario de Firefox (recomendado), asegúrese de instalar el excelente complemento *Google Sharing*, que mantiene su anonimato mientras realiza una búsqueda en Google. Incluso si no usa Google, debe cuidarse de un gran número de sitios web que utilizan una barra personalizada de búsqueda de Google como un medio para explorar su contenido

Por lo dicho anteriormente, no se puede confiar en Google, en Yahoo ni en Bing. Nosotros recomendamos cambiar por un servicio de búsqueda que toma en cuenta su derecho a la privacidad muy seriamente: DuckDuckGo (<http://duckduckgo.com/>).

## Más ojos de los que usted puede ver

Internet es un enorme lugar y no es una única red, sino que es una gran red formada por muchas redes pequeñas interconectadas entre sí. Cuando usted solicita una página a un servidor

---

de Internet su solicitud puede atravesar muchas máquinas antes de alcanzar al servidor que hospeda la página. Este trayecto se conoce como encaminamiento y típicamente incluye al menos 10 máquinas a través de la ruta. Como los paquetes se mueven de una máquina a otra, deben copiarse en la memoria, reescribirse y traspasarse.

Cada una de las máquinas a través del encaminamiento en la red pertenece a alguien, normalmente una empresa u organización y puede estar en diferentes países. Si bien se están realizando esfuerzos para estandarizar las leyes de comunicación entre los países, existe en la actualidad una amplia variedad según la jurisdicción. Así, mientras que puede que no haya una ley que exige el registro de su navegación por la web en su país, tales leyes pueden existir en otro lugar a lo largo de la ruta de su paquete.

La única forma de proteger el tráfico a lo largo de la ruta de que sea grabado o manipulado es utilizar cifrado de extremo a extremo como el proporcionado por TLS/Secure Socket Layer (Vea el capítulo **Cifrado**) o una red privada virtual (Vea el capítulo **VPN**).

## **Su derecho a permanecer en el anonimato**

Más allá del deseo de minimizar las fugas de privacidad para los proveedores de servicios específicos, usted debe considerar ocultar la dirección de Internet desde la cual se conecta habitualmente (vea el capítulo **Qué sucede cuando navega**). El deseo de lograr este anonimato impulsó la creación del *Proyecto Tor*.

*Tor* usa una red de nodos en constante evolución para enrutar

la conexión a un sitio de una manera que no se puede rastrear de nuevo hasta usted. Es un medio muy robusto para asegurar que su dirección de Internet no se puede registrar en un servidor remoto. Vea el capítulo **Anonimato** para obtener más información acerca de cómo funciona y cómo empezar con Tor.

# 15

## Temores

### Redes sociales - ¿cuáles son los peligros?

El fenómeno de las redes sociales han cambiado no sólo a la forma en cómo la gente usa Internet. Grandes servidores alrededor del mundo, particularmente en EEUU, se han construido para atender al deseo repentino y enorme de la gente de subir contenido sobre sí mismos, sus intereses y sus vidas con el fin de participar en las redes sociales.

Las redes sociales, tal como conocemos a Facebook, Twitter (y anteriormente MySpace) están lejos de ser “libres”. Más bien, se trata de empresas que buscan desarrollarse sobre una angustia muy básica para luego poder explotarla: el miedo a la irrelevancia social. Como animales sociales que somos no podemos soportar la idea de aislarnos y por lo tanto muchos se creen integrados colocando sus expresiones más íntimas en el disco duro de un hombre de negocios, enclavado en un centro de datos en otro país - uno que nunca se le permitirá visitar.

A pesar de esto, muchos podrían argumentar que el calor social y el reconocimiento personal adquirido a través del compromiso con las redes sociales, compensa la posible pérdida de la privacidad. Tal afirmación, sin embargo es válida sólo cuando se conoce completamente la magnitud de los riesgos.

Las amenazas de las redes sociales al derecho básico de las personas a la privacidad son las siguientes:

- El alcance y la intimidad de las contribuciones individuales de los usuarios.
- Un usuario que publica frecuentemente e incluye muchos detalles personales construye un cuerpo de información de enorme utilidad para marketing directo.
- La preparación del usuario para asumir riesgos sociales.
- Un usuario que establece conexiones sociales sin cuidado corre un gran riesgo ante ataques de ingeniería social y los depredadores.
- Los intereses económicos y los socios de las organizaciones que proveen el servicio.
- Estudios encargados de clientes, minería de datos, análisis de sentimientos.
- Demandas político/legales ejercidas por el Estado contra la organización en las jurisdicciones en las cuales reside.
- Órdenes de los jueces para obtener datos de un usuario particular (sin importar si es nativo o extranjero).
- Agendas de vigilancia por aplicación de leyes o socios de la organización.
- Análisis de sentimientos: proyecciones de intentos políticos.

Con estas cosas en mente, es posible señalar un gran contraste entre proyectos como Diáspora y Facebook: el primero promete

---

un cierto nivel de transparencia organizativa, el compromiso con la privacidad y una apertura general, mientras que Facebook ha demostrado ser una empresa turbia económicamente capaz de especular con la privacidad de sus usuarios y gestionar demandas civiles antes que lo hagan sus clientes. Por lo tanto es más probable de que su reputación sea analizada por una compañía de seguros o un empleador potencial si usa la gran red social en lugar de otra más pequeña y transparente.

## ¿Quién puede robar mi identidad?

La respuesta depende del contexto en el cual usted trabaja con su navegador. Una contraseña débil y única para múltiples servicios de redes sociales, banca, webmail, etc. es muy peligrosa y es muy factible que sea robada. Una contraseña fuerte y única en una red inalámbrica compartida con otros (ya sea abierta o cifrada) es vulnerable. La regla general es que usted se asegure de tener una contraseña personal fuerte (ver la sección de **Contraseñas**).

## Redes inalámbricas

Aquí nos encontramos en medio de un riesgo a menudo subestimado de que alguien escuche nuestras comunicaciones usando un *paquete de sniffing de red*. Poco importa si la red es abierta o posee una contraseña segura. Si alguien utiliza la misma red cifrada, puede fácilmente capturar y leer todo el tráfico inseguro de otros usuarios en la misma red. Una clave inalámbrica puede ser adquirida por el costo de una taza de café y le da a todos aquellos que saben cómo capturar y leer los paquetes de red la oportunidad de leer su contraseña mientras usted revisa su correo electrónico.

Existe una regla simple que debe aplicarse siempre: si el café ofrece una conexión de cable de red, ¡úsela! Finalmente, así como en un cajero automático, asegúrese de que no miran por encima del hombro cuando escribe la contraseña.

## El caché del navegador web

Debido a la molestia general de tener que escribir su contraseña en repetidas ocasiones, muchas personas permiten que el navegador o el cliente de correo local lo almacenen por usted. Esto no es malo en sí mismo, pero cuando un ordenador portátil o teléfono es robado, le permite al ladrón acceder a la cuenta del propietario del correo electrónico. Lo más recomendable es limpiar la caché siempre que cierre su navegador. Todos los navegadores populares tienen una opción para borrar la memoria caché al salir.

El uso de la memoria caché se justifica si toma la precaución de cifrar su disco. Si su dispositivo portátil es robado y el ladrón reinicia la máquina, van a encontrarse con un disco cifrado. También es aconsejable tener un bloqueo de pantalla instalado en su ordenador o teléfono. Si la máquina es robada mientras está ejecutando una sesión de usuario, no se podrá acceder a ella.

## Asegurando su línea

Mientras esté registrado en cualquier servicio debería asegurarse de usar cifrado para la sesión completa. Esto se puede hacer fácilmente con el popular *TLS/SSL (Secure Socket Layer)*.

Compruebe que el servicio que está usando (ya sea correo electrónico, redes sociales o banca en línea) es compatible con sesiones TLS/SSL viendo la existencia de <https://> al comienzo

---

de la URL. Si no es así, asegúrese de activarlo en todas las configuraciones proporcionadas por el proveedor del servicio. Para entender mejor cómo funciona la navegación web, consulte el capítulo **¿Qué sucede cuando navego en Internet?**

## **¿Puedo meterme en problemas por usar Google con cosas raras?**

Google y otras compañías de búsqueda pueden cumplir con las órdenes judiciales dirigidas a determinadas personas. Un sitio web con un campo personalizado de búsqueda de Google para encontrar contenido en su sitio puede ser obligado a registrar y suministrar todas las consultas de búsqueda a la justicia local. Académicos, artistas e investigadores están particularmente en riesgo de ser mal entendidos, ya que suponen motivaciones donde sólo existen intereses aparentes.

## **¿Quién mantiene un registro de mi navegación? ¿puedo esconderme de ellos?**

Está completamente cubierto por sus derechos humanos básicos, y comúnmente protegido constitucionalmente, para poder visitar los sitios web de forma anónima. Del mismo modo que se le permita visitar una biblioteca pública, hojear libros y ponerlos de nuevo en la estantería sin que nadie tome nota de las páginas y los títulos de su interés, usted es libre de navegar de forma anónima en Internet.

## *¿Cómo hacer para no revelar mi identidad?*

Consulte el capítulo sobre **Anonimato**.

## *¿Cómo evitar ser rastreado?*

Vea el capítulo de **Seguimiento**.

# 16

## Qué sucede cuando usted navega

Navegar por la web es comunicarse. Puede que usted no envíe mucho texto en términos de cantidad de palabras, pero siempre es el navegador el que inicia y mantiene la comunicación al solicitar los bits y las piezas de datos que están involucrados con lo que usted eventualmente ve en su pantalla.

Los navegadores tales como Mozilla Firefox, Google Chrome, Opera, Safari e Internet Explorer trabajan todos de manera similar. Cuando escribe una URL (por ejemplo “<http://happybunnies.com>”) en la barra de direcciones, el navegador solicita el sitio web (el cual es sólo un tipo especial de texto) de un servidor remoto y entonces lo transforma en bloques coloridos, textos e imágenes para ser mostrados en la ventana del navegador. Para ver el texto de la manera en que el navegador lo ve, sólo debe hacer click en **Ver --> Código de la página**. Lo que verá será la misma página web pero en HTML – un lenguaje que se ocupa principalmente del contenido, el contexto y los enlaces a otros recursos (CSS y JavaScript) que gobiernan la forma en que los contenidos son mostrados y cómo se comportan.

Cuando el navegador intenta abrir una página web - y

suponiendo que no hay proxies involucrados - lo primero que hace es comprobar su propia caché. Si no tiene registros de visitas anteriores a dicho sitio, intentará resolver el nombre en una dirección que realmente puede utilizar. Se trata de un programa de internet, por lo que necesita una dirección de Protocolo de Internet (dirección IP o simplemente IP). Para obtener esta dirección se le pide a un servidor DNS (una especie de guía telefónica para los programas de Internet) que se instala en el router de su conexión a internet de forma predeterminada<sup>1</sup>. La dirección IP es una etiqueta numérica asignada a cada dispositivo en la red (global), como la dirección de una casa en el sistema postal - y como la dirección de su casa, usted debe tener mucho cuidado a quién se la da (por defecto es visible para todos). Una vez que la dirección IP ha sido recibida, el navegador abre una conexión TCP (un protocolo de comunicación) al host de destino y comienza a enviar paquetes a un puerto en esta dirección, por lo general el puerto 80 (los puertos son como puertas a los servidores, hay muchos, pero por lo general sólo unos pocos están abiertos)<sup>2</sup> a menos que se especifique otra ruta. Estos paquetes viajan a través de una serie de servidores en Internet (hasta un par de docenas en función de donde se encuentra la dirección de destino). Después, el servidor busca la página solicitada y, si lo encuentra, la entrega utilizando el protocolo HTTP. (Para evitar que otras personas lean o alteren los datos, se debe usar TLS/SSL junto con HTTP para asegurar la conexión).

Cuando llega la respuesta HTTP, el navegador puede cerrar la conexión TCP o reutilizarlo para las solicitudes posteriores. La respuesta puede ser una entre muchas, desde algún tipo de redirección hasta el clásico error interno del servidor (500). Siempre que la respuesta es la esperada, el navegador guarda la página en la memoria caché para su uso posterior, la decodifica (la descomprime si está comprimida, la renderiza si es un códec de vídeo, etc) y la muestra en pantalla o la ejecuta de acuerdo con

---

las instrucciones.<sup>3</sup>

Ilustremos el proceso con una pequeña conversación entre el navegador (B) y el servidor (S):

B: “Hola.”

S: “Hola!”

B: “¿Puede alcanzarme la página con los conejitos felices, por favor?”

S: “Bien, aquí la tiene.”

B: “Oh, tal vez usted podría alcanzarme una versión más grande de esa imagen en la cual el conejito bebé abraza un oso de peluche.”

S: “Seguro, por qué no.”

[...]

B: “Esto es todo por ahora. Muchas gracias. Adiós.”

Tenga en cuenta que hay un montón de actividades que suceden paralelamente a este intercambio de TCP/IP. Dependiendo de cómo haya configurado las opciones, el navegador podría añadir la página a la historia del navegador, guardar cookies, comprobar plugins y actualizaciones RSS y comunicarse con una gran variedad de servidores, todo mientras está haciendo otra cosa.

## Una topografía suya: huellas

Lo más importante: siempre dejará rastros. Algunos permanecerán en su propia computadora – una colección de datos en caché, la historia de navegación y pequeños archivos malvados con memoria de elefante llamados cookies. Son todos ellos muy ventajosos; aceleran su navegación, reducen su descarga de datos o recuerdan sus contraseñas y preferencias en

las Redes Sociales. También estudian sus hábitos de navegación y recopilan registros de todos los lugares que visita y de todo lo que hace en ellos. Esto debería preocuparlo si está usando una computadora pública en una biblioteca, en su trabajo o en un cibercafé, o si comparte el departamento con un compañero entrometido.

Incluso si configura su navegador para no registrar el historial de navegación, rechaza las cookies y borra los archivos almacenados en caché (o asignar cero MB de espacio en caché), seguiría dejando rastros por toda Internet. Su dirección IP queda registrada de forma predeterminada en todas partes y para todo el mundo y los paquetes enviados son supervisados por un número cada vez mayor de entidades - comerciales, gubernamentales o criminales, junto con algunos cretinos y acosadores potenciales.

Los gobiernos democráticos en todas partes están rediseñando las regulaciones para exigir a los proveedores de Internet que conserven una copia de todo para poder tener acceso a ella más tarde. En los EE.UU., el artículo 215 de la Ley Patriótica Estadounidense '*prohíbe a un individuo u organización revelar que les ha dado sus registros al gobierno federal, siguiendo una investigación*'. Eso significa que la empresa a la cual usted le paga cada mes para poder tener acceso a Internet puede ser obligada a entregar su historial de navegación y sus registros de correo electrónico sin su conocimiento.

La mayor parte del tiempo, sin embargo, la vigilancia no es un asunto de 1984. Google recopila sus búsquedas, junto con su identificación del navegador (*user agent*), su dirección IP y un montón de datos que eventualmente puede conducir a su puerta, pero el objetivo final no suele ser la represión política, sino la investigación de mercado. Los anunciantes no se preocupan solamente por el espacio publicitario, ellos quieren saberlo todo sobre usted. Ellos quieren saber sus hábitos de medicación y dietarios, el número de hijos que tiene y dónde se toman las va-

---

caciones, qué hace con su dinero, cuánto gana y cómo le gusta gastarlo. Aún más: quieren saber qué *sienten* acerca de determinadas cosas. Ellos quieren saber si sus amigos respetar esos sentimientos lo suficiente para que pueda convencerlos de que cambien sus hábitos de consumo. Esto no es una conspiración, sino más bien la naturaleza del capitalismo en la era de la información. Parafraseando una famosa observación de la situación actual, las mentes más brillantes de nuestra generación está pensando en cómo hacer que la gente haga click en los avisos comerciales.<sup>4</sup>

Algunas personas piensan que los avisos comerciales pueden ignorarse o que los publicistas satisfacen nuestras necesidades específicas en una situación de ganar-ganar, porque el spam que reciben se refiere a cosas que eventualmente desean. Si este fuera el caso (y no lo es): ¿deberíamos confiarle a Google aspectos íntimos y detallados de nuestra vida? Aunque creamos que Google ‘no es el diablo’, puede ser comprado por alguien en quien no confiamos; los benevolentes Larry Page y Sergey Brin pueden ser destituidos por su propio Consejo, o su base de datos puede ser secuestrada por un gobierno fascista. Uno de sus 30.000 empleados en todo el mundo puede irse con nuestros datos. Sus servidores pueden ser hackeados. Después de todo, sólo están interesados en sus clientes, *las empresas que pagan por publicidad*. Sólo somos el producto que se vende.

Más aún; en las Redes Sociales nuestros hábitos de navegación generan un registro permanente, una colección de datos tan vasta que la información que Facebook recopila acerca de un sólo usuario puede llenar 880 páginas. Nadie podrá sorprenderse al saber que el propósito de Facebook no es hacernos más felices – de nuevo: si usted no paga por algo, no es un cliente, es el producto. Pero aunque no le preocupen sus objetivos comerciales, piense en esto: la plataforma tiene publicidades que permiten que hackers maliciosos irrumpan en cientos de miles de cuentas de Facebook todos los días.

Para una muestra de lo que se esconde detrás de las cortinas de los sitios web que visita, instale un plugin/add-on llamado *Ghostery* en tu navegador. Es como una radiografía de la máquina que revela toda la tecnología de vigilancia que puede estar (y a menudo lo está) incrustada en una página web, normalmente invisible para el usuario. En esta misma línea, *Do Not Track Plus* y *Trackerblock* le darán un mayor control sobre el seguimiento online, a través del bloqueo de cookies, las cookies persistentes opt-out, etc. Nuestro capítulo siguiente **Seguimiento** le enseñará mucho acerca de dichos temas.

Incluso entre el ordenador y el router, los paquetes pueden ser fácilmente interceptadas por cualquier persona que utilice la misma red inalámbrica en el ambiente informal de un café. Es una jungla allá afuera, pero todavía elegimos contraseñas como “password” y “123456”, realizamos transacciones económicas y compramos entradas en las redes públicas inalámbricas y hacemos click en enlaces de correos electrónicos no solicitados. No se trata solamente de nuestro derecho a preservar nuestra intimidad, también tenemos la responsabilidad de defender ese derecho contra las intrusiones de los gobiernos, empresas y cualquier persona que intentan despojarnos de ellos. Si no ejercemos esos derechos hoy en día, nos merecemos lo que suceda mañana.

1. Si es un usuario de Unix, puede usar el comando `tcpdump` en el bash y ver el tráfico dns en tiempo real. ¡Está cargado de diversión! (y disturbios) ^
2. Vea la lista de números de puertos TCP y UDP ([https://es.wikipedia.org/wiki/Anexo:Lista\\_de\\_números\\_de Puerto](https://es.wikipedia.org/wiki/Anexo:Lista_de_números_de Puerto)). ^
3. Si el intercambio se produce bajo una conexión HTTPS, el proceso es mucho más complicado y también mucho más seguro, hallará más información acerca de esto en el fascinante capítulo llamado Criptografía. ^
4. This Tech Bubble Is Different (<http://www.businessweek.com/magazine/content>) ^ Cuentas y se-

---

## guridad =====

Cuando navega por Internet, puede estar conectado con varios servicios, a veces en forma simultánea. Puede estar en el sitio web de una empresa, viendo su correo electrónico o en una red social. Nuestras cuentas son importantes porque almacenan información altamente sensible acerca de nosotros y de otras personas en máquinas a lo largo de toda Internet.

Mantener sus cuentas seguras requiere algo más que una contraseña segura (véase la sección **Contraseñas**) y un vínculo de comunicación segura con el servidor a través de TLS/SSL (véase el capítulo **Conexión segura**). A menos que se especifique lo contrario, la mayoría de los navegadores almacenan sus datos de acceso en pequeños archivos llamados cookies, reduciendo la necesidad de volver a escribir la contraseña cuando vuelva a conectarse a estos sitios. Esto significa que alguien con acceso a su computadora o teléfono celular puede acceder a sus cuentas sin tener que robar la contraseña o hacer espionaje sofisticado.

Desde que los teléfonos inteligentes se han vuelto muy populares ha habido un aumento dramático en el secuestro de cuentas por robo de teléfonos. El robo de computadoras portátiles presenta un riesgo similar. Si usted elige que el navegador guarde sus contraseñas entonces usted tiene varias opciones para protegerse:

- Utilice un bloqueo de pantalla. Si usted tiene un teléfono y prefiere un sistema de patrón de desbloqueo debe adquirir el hábito de limpiar la pantalla para que un atacante no pueda adivinar el patrón de manchas de los dedos. En una computadora portátil, debe configurar su salvapantallas para que le pida una contraseña, así como una contraseña en el arranque.
- Cifrar el disco duro. TrueCrypt es un sistema de cifrado de disco abierto y seguro para Windows 7/Vista/XP, Mac OS X y GNU/Linux. OSX y muchas distribuciones de GNU/Linux ofrecen la opción de cifrado de disco en la

instalación.

- Desarrolladores Android: no habilitar la depuración USB en el teléfono de forma predeterminada. Esto permite a un atacante utilizar el *adb shell* de Android en una computadora para acceder al disco duro de su teléfono sin desbloquearlo.

## ¿Puede un sitio web malicioso apoderarse de mis cuentas?

Aquellos cookies especiales que contienen sus datos de inicio de sesión son el punto primario de vulnerabilidad. Una técnica muy popular para robo de datos es el llamado clickjacking, donde el usuario es engañado al hacer click en un enlace aparentemente inofensivo, ejecutando un script que se aprovechará del hecho de que usted está logueado. Los datos de inicio de sesión pueden ser robados, permitiéndole al atacante remoto acceder a su cuenta. Aunque es una técnica complicada, ha probado ser muy efectiva en varias ocasiones. Tanto en Twitter como en Facebook se han registrado casos de inicio de sesión robadas usando esta técnica.

Es importante desarrollar hábitos para pensar antes de hacer click en enlaces a sitios mientras está logueado en sus cuentas. Una técnica es utilizar otro navegador que no registre las cuentas como una herramienta para probar la seguridad de un enlace. Confirme siempre la dirección (URL) en el enlace para asegurarse de que esté escrita correctamente. Puede ser un sitio con un nombre muy similar al del sitio en el cual confía. Tenga en cuenta que los enlaces con acortadores de URL (como <http://is.gd> y <http://bit.ly>) son riesgosos ya que no puede ver el enlace real al cual usted está solicitando los datos.

Si utiliza Firefox en su dispositivo, utilice el complemento No-Script, ya que mitiga muchas de las técnicas de *Cross Site Script-*

---

*ing* que permitan que su cookie de login sea robado, pero tenga en cuenta que se deshabilitarán muchas características de algunos sitios web.

Qué sucede cuando usted navega

# 17

## Seguimiento

Cuando navega por la web pequeños rastros de su presencia van quedando por el camino. Muchos sitios web inofensivos usan estos datos para compilar estadísticas y ver cuánta gente está visitando el sitio y qué páginas son populares, pero algunos sitios usan estas técnicas para rastrear usuarios individuales, tratando de ir más allá para identificarlos personalmente. Sin embargo, no se detienen acá. Algunas empresas almacenan datos en su navegador para registrarlos a usted en otros sitios. Esta información puede ser recopilada y pasada a otras organizaciones sin su conocimiento o permiso.

Todo esto suena ominoso ¿pero a quién le importa realmente si alguna gran empresa sabe de unos pocos sitios web que hemos visto? Los sitios web grandes recopilan y utilizan estos datos para “publicidad comportamental” donde los anuncios están diseñados para satisfacer exactamente sus intereses. Es por eso que después de mirar la entrada de Wikipedia para Mallorca, uno de repente puede comenzar a ver un montón de anuncios para la paquetes de vacaciones envasados y sombreros de fiesta. Esto puede parecer bastante inocente, pero después de hacer una búsqueda de “tratamientos para el herpes” o “comunidades

fetiche” y ver listados de repente a los productos pertinentes, se puede empezar a sentir que la web se está volviendo demasiado familiar.

Esta información es también de interés para otros, como su compañía de seguros. Si ellos saben que usted ha estado buscando en los sitios de paracaidismo o en los foros de enfermedades congénitas, sus primas misteriosamente puede empezar a aumentar de precio. Los empleadores potenciales o los propietarios de alquileres pueden perder interés basado en sus intereses en la web. En casos extremos, las autoridades policiales o fiscales pueden empezar a observarlo sin que siquiera haya cometido un delito, simplemente sobre la base de sospechas.

## ¿Cómo lo siguen?

Cada vez que carga una página web, el software del servidor en el sitio web genera un registro de la página vista en un archivo de log. Esto no es siempre una mala idea. Cuando se loguea en un sitio web, es necesario establecer su identidad y mantener registros ordenados para grabar sus preferencias, o presentarle información personalizada. Esto se logra pasándole un pequeño archivo a su navegador y almacenando una referencia correspondiente en el servidor web. Este archivo se denomina *cookie*. Suena hermoso, pero el problema es que esta información se mantiene en el equipo incluso después de salir del sitio web y podrá llamar a casa para decirle al dueño de la cookie acerca de otros sitios web que está visitando. Algunos sitios importantes, como Facebook y Google han sido descubiertos usándolos para realizar un seguimiento de su navegación, incluso después de haber cerrado la sesión.

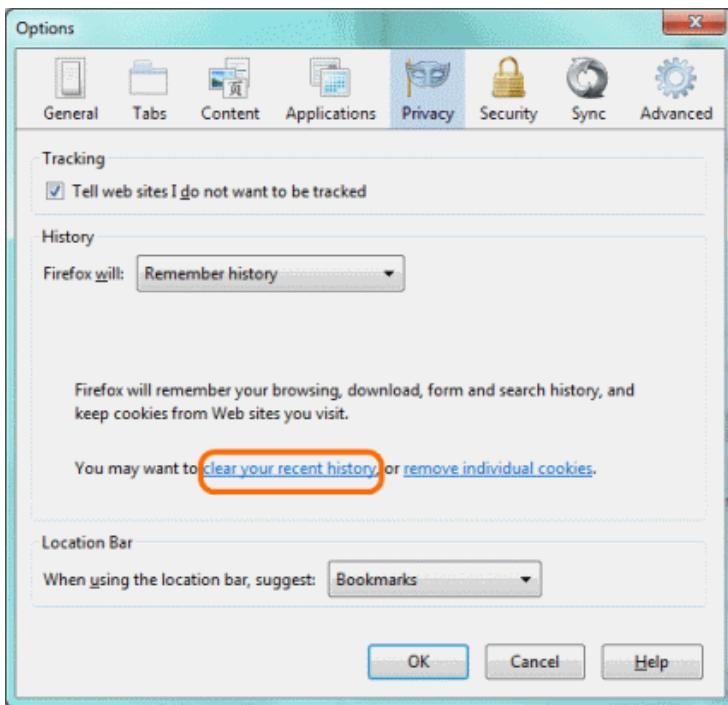
---

## ¿Cómo puedo evitar el seguimiento?

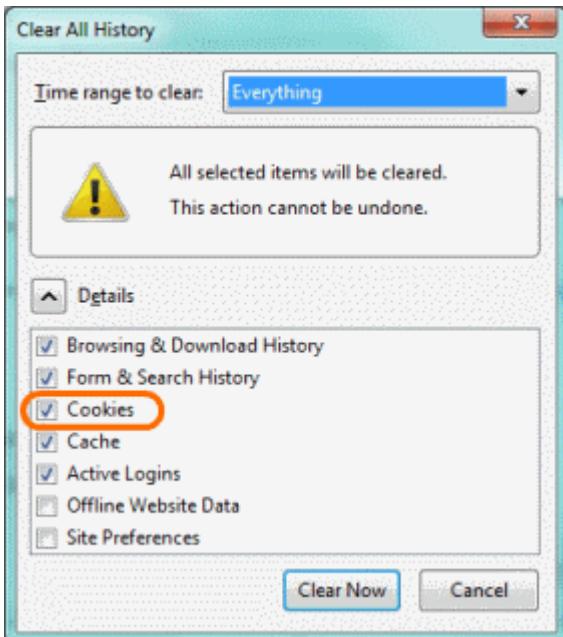
La manera más simple de evitar el seguimiento es borrar las cookies en su navegador.

En Firefox:

1. Pulse **Firefox menu**.
2. Pulse **Options**.
3. Pulse **Privacy**.
4. Pulse **Clear your recent history**.



5. Asegúrese de configurar **Time range to clear** como **Everything**.
6. Tilde **Cookies**.



7. Haga click en **Clear now**.

En **Chrome**: 1. Pulse **Chrome menu**. 2. Pulse **Tools**. 3. Pulse **Clear browsing data**. 4. Asegúrese de configurar **Obliterate the following items from** como **The beginning of time**. 5. Tilde **Delete cookies and other site and plug-in data**. 6. Pulse **Clear browsing data**.

En **Internet Explorer**: 1. Pulse el botón **Tools** (en forma de engranaje). 2. Pulse **Safety**. 3. Pulse **Delete Browsing History**. 4. Tilde **Cookies**. 5. Pulse **Delete**.

La limitación de esta aproximación es que usted recibirá nuevas cookies tan pronto como vuelva al sitio o cuando vaya a otras páginas con componentes de seguimiento. Otras desventajas son que usted perderá todas sus sesiones iniciadas para todas sus

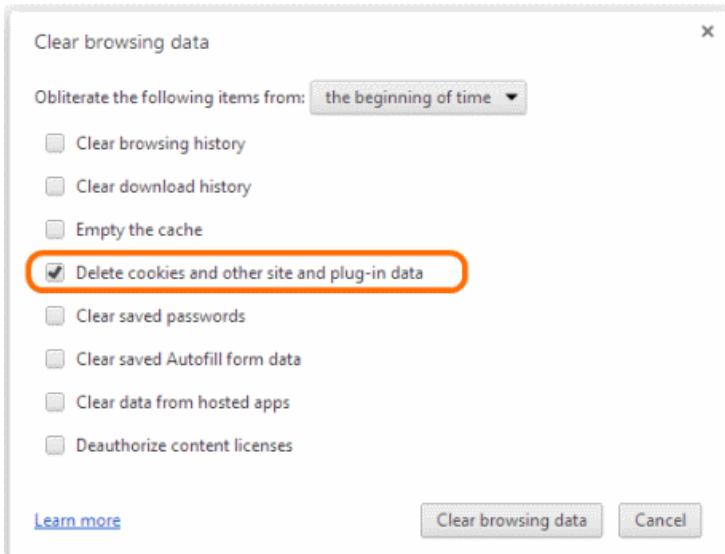


Figure 17.1: Borrado de cookies en Chrome

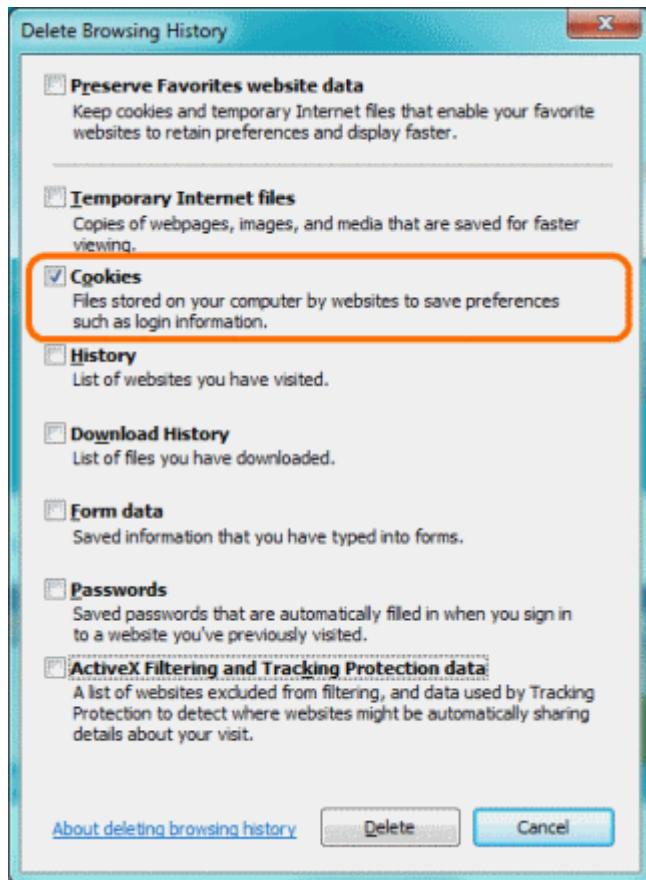
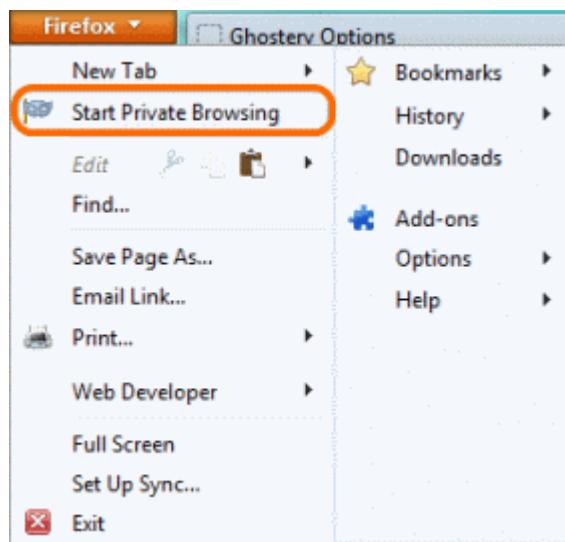


Figure 17.2: Borrado de cookies e Internet Explorer

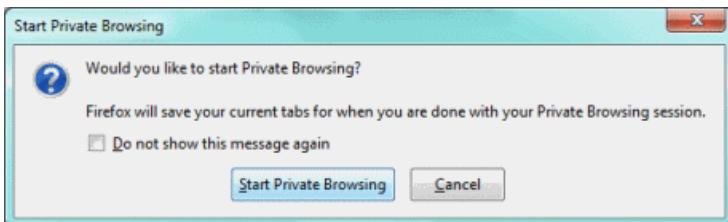
---

pestañas abiertas, forzándolo a tipar sus nombres de usuario y contraseña nuevamente. Una opción más conveniente, soportada por los navegadores actuales es navegación privada o modo incógnito. Esto abre una ventana de un navegador temporario que no grabará la historia de las páginas visitadas, contraseñas, archivos descargados o cookies. Después de cerrar la ventana de navegación privada, toda la información será borrada.

En Firefox: 1. Pulse **Firefox menu**. 2. Pulse **Start Private Browsing**.



3. Si se lo solicita, pulse **Start Private Browsing** nuevamente.



4. El botón **Firefox menu** aparece en color púrpura, mostrando que se está navegando en forma privada.

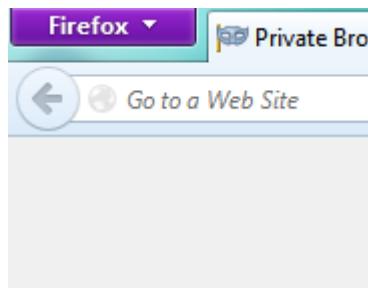
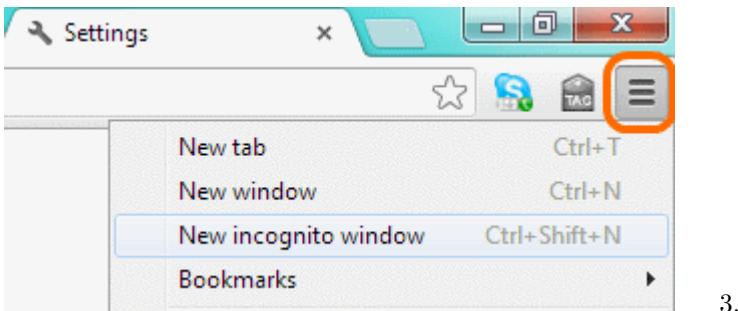


Figure 17.3: Navegación privada en Firefox

En Chrome: 1. Pulse **Chrome menu**. 2. Pulse **New incognito window**.



3.

El ícono espía en la parte superior izquierda de la ventana del

---

navegador muestra que se está navegando en forma privada.

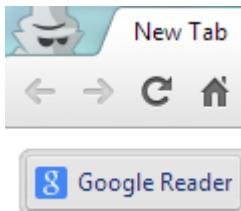
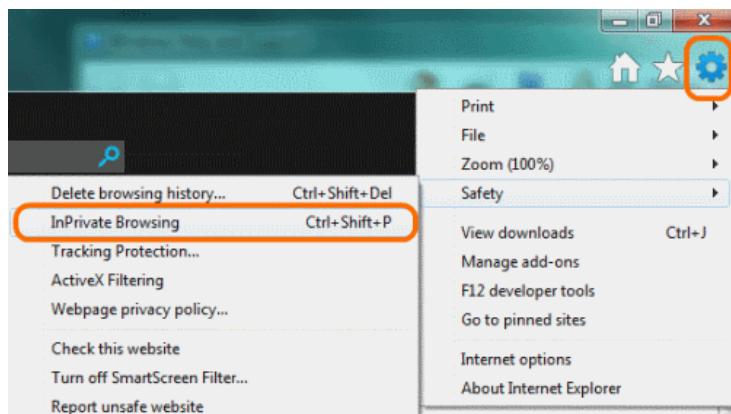


Figure 17.4: Navegación privada en Chrome

En **Internet Explorer**: 1. Pulse en el menú **Tools**, en forma de engranaje. 2. Pulse **Safety**. 3. Pulse **InPrivate Browsing**.



4. El logo **InPrivate** aparecerá en la parte superior izquierda de la ventana del navegador: se está navegando en forma privada.

Esta solución también tiene sus limitaciones. Nosotros no podemos grabar marcadores, registrar contraseñas, o sacar ventajas de la conveniencia ofrecida por navegadores modernos. Afortunadamente, existen distintos plugins especialmente diseñados

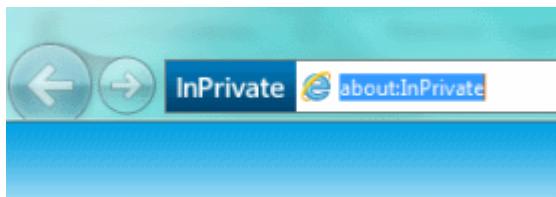
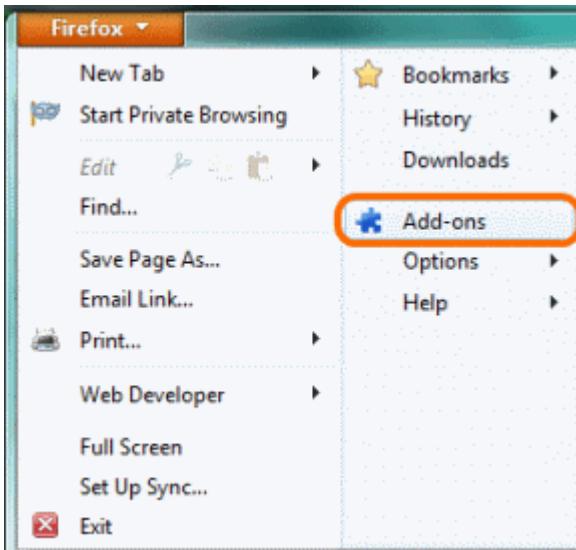


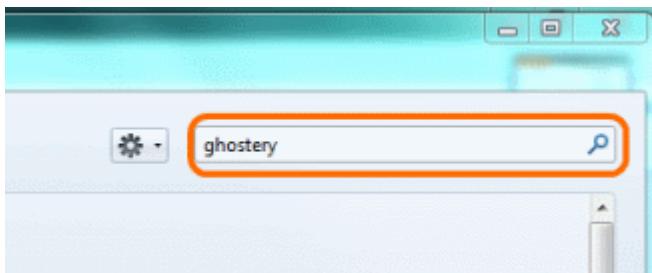
Figure 17.5: Navegación privada en IE

para direccionar los problemas del seguimiento. El más extenso, en términos de características y flexibilidad, es Ghostery. El plugin le permite bloquear servicios individuales o por categorías que registran usuarios.

1. En Firefox, pulse el menú **Firefox** y elija **Add-ons**.



2. En la casilla **Search**, tipee “ghostery”, luego pulse el ícono **Search** o presione **Enter**.



3.

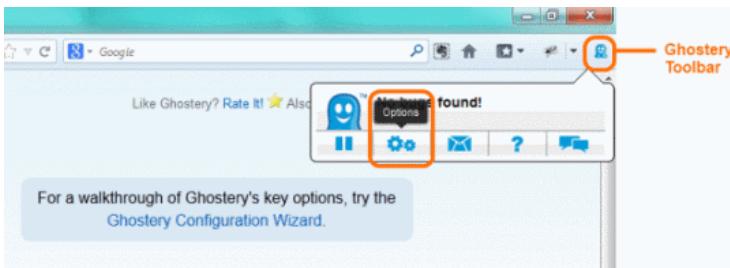
Busque Ghostery en la lista de Add-ons, y pulse **Install**.

Add-on	Last Updated	Action
Ghostery 2.8.4	Tuesday, 8 January 2013	<a href="#">More</a> <a href="#">Install</a>
Flashblock 1.5.15.1	Sunday, 17 July 2011	<a href="#">More</a> <a href="#">Install</a>
Webutation - Reputation & Security 1.0.5	Wednesday, 10 August 2011	<a href="#">More</a> <a href="#">Install</a>
Search by Image for Google 1.2.0	Thursday, 5 April 2012	<a href="#">More</a> <a href="#">Install</a>

4. Reinicie su navegador pulsando **Restart Now**.

✓ Ghostery will be installed after you restart Firefox. [Restart now](#) [Undo](#)

5. Pulse **Ghostery toolbar** y seleccione **Options**. Recorre las opciones y prueba diversos ajustes para Ghostery, si así lo deseas.



6. Visite una página web y observe sus rastreadores.

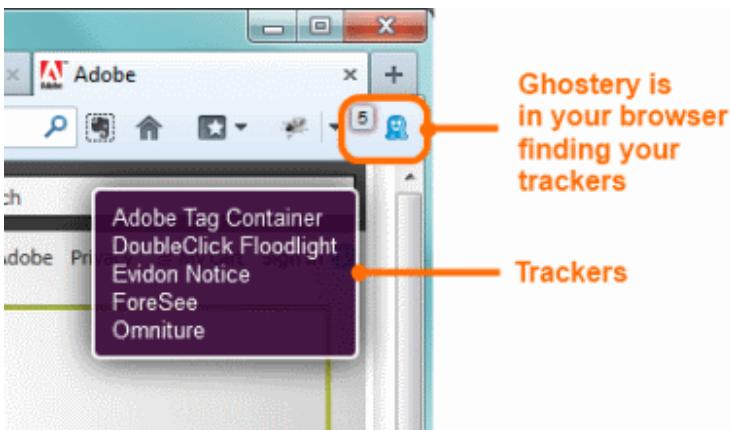


Figure 17.6: Ghostery

Otra opción es instalar un plugin bloqueador de publicidad como AdBlockPlus. Este plugin automáticamente bloqueará muchos de las cookies de seguimiento enviadas por empresas de publicidad pero no los utilizados por Google, Facebook y otras empresas de análisis web.

---

## **¿Cómo puedo ver quién me está siguiendo?**

La forma más fácil de ver quién lo está rastreando es usar el plugin Ghostery. Hay un pequeño ícono en la esquina superior derecha o inferior derecha de la ventana del navegador que le dirá qué servicios lo están siguiendo a usted en un sitio web específico.

(Sugerencia: Añada el complemento Do Not Track de Abine.com Sugerimos utilizar tanto Ghostery como DNT, porque a veces bloquean cookies distintas. Abine también tiene Privacy Suite, recientemente desarrollado que puede darle un proxy telefónico y de correo electrónico, similar a 10 Minute Mail o Guerrilla Mail para llenar correos electrónicos para formularios.)

## **Una palabra de advertencia**

Si bloquea a sus rastreadores tendrá un elevado nivel de privacidad cuando navegue por la web. Sin embargo, las agencias de gobierno, los jefes, los hackers y los administradores de red inescrupulosos aún podrán interceptar su tráfico y averiguar qué está viendo. Si quiere asegurar su conexión, necesitará leer el capítulo de cifrado. Su identidad puede ser visible para otras personas en internet. Si quiere proteger completamente su identidad mientras navega, tendrá que dar algunos pasos más hacia el anonimato en línea que se explican en otra sección de este libro.

Seguimiento

# 18

## Anonimato

### Introducción

Artículo 2 de la Declaración Universal de los Derechos Humanos:

“Toda persona tiene todos los derechos y libertades proclamados en esta Declaración, sin distinción alguna, por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición.

Además, no se hará distinción alguna en función de la condición política, jurídica o internacional del país o territorio del cual dependa una persona, tanto si es independiente, fiduciaria, no autónomo o bajo cualquier otra limitación de soberanía“.

Una forma de aplicación de este derecho básico en ambientes hostiles es por medio del anonimato, donde los intentos para conectar un agente activo a una persona específica están bloqueados.

Actuar anónimamente es también de gran ayuda para aquellos con una gran necesidad de protección - cuanto más grande es el rebaño de ovejas, más difícil es encontrar una en particular. Una manera fácil de hacerlo es mediante el uso de TOR, una técnica que enruta el tráfico de Internet entre los usuarios de un software especial, por lo que es imposible de rastrear a cualquier dirección IP específica o persona sin que tenga autoridad sobre toda la red (y que nadie tiene aún en el caso de la Internet). Un medio muy funcional para proteger la identidad de los propios es el uso de servidores proxy anónimos y redes privadas virtuales (VPN).

## Proxy

“Un **anonymizer** o un **proxy anónimo** es una herramienta que ayuda a hacer que la actividad en Internet no pueda ser rastreada. Es una computadora que es un proxy [servidor] que actúa de intermediaria y como escudo de la privacidad entre un cliente y el resto de internet. Accede a Internet en representación del usuario, protegiendo su información personal al ocultarla información que pudiera identificar a la computadora del cliente.” (<http://en.wikipedia.org/wiki/Anonymizer>)

El objetivo principal detrás del uso de un proxy es ocultar o cambiar la dirección de Internet (dirección IP) asignada a la computadora del usuario. Puede haber varias razones por las que necesitan hacerlo, por ejemplo:

- Para acceder en forma anónima a determinados servidores y/o para ocultar los rastros que quedan en los archivos de registro de un servidor web. Por ejemplo, un usuario podría necesitar acceder a materiales sensibles en línea

---

(materiales especiales, temas de investigación u otra cosa) sin llamar la atención de las autoridades.

- Para atravesar los cortafuegos de las empresas o de los regímenes represivos. Un gobierno/corporación puede limitar o restringir completamente el acceso a Internet a una dirección IP específica o un rango de direcciones IP. Al esconderse detrás de un proxy ayudará a engañar a estos filtros y acceder a sitios prohibidos de otra manera.
- Para ver los videos online prohibidos en su país debido a cuestiones legales.
- Para acceder a los sitios web y/o materiales disponibles sólo para las direcciones IP que pertenecen a un país específico. Por ejemplo, un usuario quiere ver un video en la BBC (Reino Unido solamente), mientras que no residen en el Reino Unido.
- Para acceder a Internet desde una dirección IP parcialmente prohibida/bloqueada. Las direcciones IP públicas a menudo puede tener “mala fama” (abuso del ancho de banda, estafa o distribución de correo electrónico no solicitado) y ser bloqueadas por algunos sitios web y servidores.

Aunque el proxy debería utilizarse para acceder a la Web (HTTP), en la práctica el protocolo de Internet puede ser “proxificado”, es decir, enviado vía servidor remoto. A diferencia de un router, un servidor proxy no envía directamente las peticiones de usuarios remotos, sino que interviene en las solicitudes y respuestas hechos a la computadora del usuario remoto.

El proxy (a menos que esté configurado como “transparente”) no permite la comunicación directa a Internet por eso las aplicaciones tales como navegadores web, clientes de chat o aplicaciones de descargas deben tenerlo en cuenta al conectarse (vea el capítulo **Navegación web segura/Configuración de proxy**)

## Tor

- Tor impide que alguien conozca su localización o aprenda acerca de sus hábitos de navegación.
- Tor funciona con navegadores web, clientes de mensajería instantánea, sesiones remotas, etc.
- Tor es software libre y está disponible para Windows, Mac, GNU/Linux, Unix y Android.  
(<https://www.torproject.org>)

Tor es un sistema destinado a permitir el anonimato en línea, compuesto por un software cliente y una red de servidores que pueden ocultar información sobre la ubicación de los usuarios y otros factores que pudieran identificarlos. Imagine un mensaje que está envuelto en varias capas de protección: cada servidor tiene que quitarle una capa, con lo que inmediatamente elimina la información del remitente del servidor anterior.

El uso de este sistema hace que sea más difícil de rastrear el tráfico en Internet del usuario, que incluye visitas a sitios web, publicaciones online, mensajes instantáneos y otras formas de comunicación. Su objetivo es proteger la libertad personal de los usuarios, la privacidad y la capacidad de hacer negocios confidencialmente, al evitar que sus actividades en Internet sean monitoreadas. El software es libre y la red de uso gratuito.

Tor no puede y no intenta protegerlo del monitoreo del tráfico que entra y sale de la red. Mientras que Tor proporciona protección contra el análisis de tráfico, no puede evitar el tráfico de confirmación (también llamado correlación de extremo a extremo). La *correlación de extremo a extremo* es una manera de hacer coincidir una identidad online con una persona real.

Un ejemplo reciente involucra al FBI que quería demostrar que un hombre, Jeremy Hammond, estaba detrás de un alias que se sabía responsable de varios ataques anónimos. Sentado frente a su casa, el FBI estaba monitoreando su tráfico inalámbrico

---

junto a un canal de chat que sabía que visitaba el alias. Cuando Jeremy se conectó en su apartamento, la inspección de los paquetes inalámbricos reveló que estaba usando Tor en el mismo momento en que el alias sospechado asociado con él se conectó al canal de chat vigilado. Esto fue suficiente para incriminar a Jeremy y él fue arrestado.

Consulte la sección **Navegación segura/Uso de Tor** para instrucciones de configuración.



# 19

## VPN

La forma en que los datos van y vuelven entre el servidor y su computadora portátil o dispositivo móvil no es tan sencilla como podría parecer. Supongamos que está conectado a una red inalámbrica en casa y abre una página, por ejemplo, wikipedia.org. La ruta de su solicitud (datos) va a consistir en múltiples puntos medios o “*saltos*” - en la terminología de arquitectura de red. En cada uno de estos saltos (probablemente más de 5) sus datos pueden ser potencialmente recogidos, copiados y modificados por:

- Su red inalámbrica (sus datos pueden ser husmeados desde el aire)
- Su ISP (en la mayoría de los países están obligados a mantener registros detallados de la actividad del usuario)
- Un Internet Exchange Point (IXP) en algún lugar en otro continente (generalmente más seguro que cualquier otro *salto*)
- El ISP de la empresa de hosting que aloja el sitio (probablemente está manteniendo registros)
- La red interna a la que está conectado el servidor
- Y varios saltos entre ...

Cualquier persona con acceso físico a las computadoras o las redes que están en el camino de usted con el servidor remoto, de forma deliberada o no, puede recoger y mostrar los datos que se pasan desde que el servidor remoto y viceversa. Esto es especialmente cierto para situaciones llamadas de “última milla” - los últimos saltos que hace una conexión a Internet para llegar a un usuario. Eso incluye redes inalámbricas o cableadas, privadas o públicas, redes móviles y telefónicas, redes en bibliotecas, hogares, escuelas, hoteles. El ISP no puede ser considerado seguro, ni una instancia ‘neutral a los datos’ - en muchos países las agencias estatales ni siquiera necesitan una orden judicial para acceder a sus datos, y siempre existe el riesgo de intrusión por parte de atacantes pagos que trabajan para adversarios de bolsillos profundos.

VPN - una red privada virtual - es una solución para esta filtración de “última milla”. VPN es una tecnología que permite la creación de una red virtual en la parte superior de una infraestructura existente. Tal red VPN funciona usando los mismos protocolos y estándares como la red física subyacente. Utiliza a los programas y al sistema operativo de forma transparente, como si se tratara de una conexión de red por separado, sin embargo, su topología o la forma en cómo los nodos de la red (usted, el servidor VPN y, potencialmente, otros miembros o servicios disponibles en VPN) están conectados entre sí en relación con el espacio físico es totalmente nueva.

Imagínese que en vez de tener que confiar sus datos a todos y cada uno de los intermediarios (su red local, ISP, el Estado) tiene la opción de pasar a través de un servidor de un proveedor VPN en quien usted confía (después de una recomendación o de una investigación) - desde el cual los datos viajarán a la ubicación remota. VPN le permite recrear su contexto local y geopolítico todo junto - desde el momento en que sus datos dejan a su equipo y se meten en la red VPN están plenamente asegurados con cifrado tipo TLS/SSL. Y como tal, aparecerá

---

como puro ruido aleatorio a cualquier nodo que podrían estar espiando detrás suyo. Es como si los datos se desplazaran dentro de un tubo de aleación de titanio, irrompible en todo el camino desde su computadora hasta el servidor VPN. Por supuesto, uno podría argumentar que con el tiempo, cuando los datos están fuera del puerto seguro de la VPN se vuelve tan vulnerables como lo eran antes - pero esto es sólo parcialmente cierto. Una vez que los datos salen del servidor VPN están lejos suyo - más allá del alcance de algunos cretinos que husmean en la red local inalámbrica, su venal ISP o un gobierno local obsesionado con las leyes antiterroristas. Un proveedor VPN serio tendría sus servidores instalados en un lugar de intercambio en Internet de alta seguridad, dificultando seriamente el acceso físico humano, la grabación o el registro.

“Todo lo que usted hace hoy en día en Internet está monitoreado y nosotros queremos cambiar esto. Con nuestro servicio de VPN rápida usted tendrá un anonimato total en Internet. Podrá navegar en sitios web censurados, que su escuela, ISP, trabajo o país están bloqueando. [DarkVPN] no solo ayudará a la gente a navegar anónimamente, también ayudará a la gente de países como China para que puedan navegar por páginas web censuradas. Lo cual es su derecho democrático. DarknetVPN le da a todos los usuarios VPN una dirección IP anónima. Todos los registros electrónicos terminarán en usted. Nosotros no grabamos ningún archivo de registros para alcanzar el máximo anonimato posible. Con nosotros usted siempre puede navegar en forma anónima, segura y cifrada.” (<http://www.darknetvpn.com/about.php>)

Otra característica interesante y a menudo subestimada de una VPN está codificada en su nombre - además de ser **Virtual** y **Privada** es también una red (**Network**). La VPN permite no

sólo conectarse por medio de su servidor al resto del mundo sino también comunicarse con otros miembros de la misma red VPN sin tener que abandonar la seguridad de su espacio cifrado. Por medio de esta funcionalidad las VPN's se convierten en algo así como una *Darknet* (en el sentido amplio de la palabra) - una red aislada de Internet e inaccesible a "otros". Ya que una conexión con un servidor VPN, y esto la red privada lo facilita, requiere una clave para *certificar*, solamente se permite a los usuarios "invitados". No existe chance de que un extraño de Internet pudiera obtener acceso a una VPN sin registrarse como usuario o sin robar alguna clave. Mientras no sea referida como tal, cualquier tipo de red intranet corporativa es también una Darknet.

"Una red privada virtual (VPN) permite una extensión segura sobre una red pública o no controlada como Internet. Permite que la computadora en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada con toda la funcionalidad, seguridad y políticas de gestión de una red privada." (<https://es.wikipedia.org/wiki/vpn>)

Muchos proveedores comerciales de VPN hacen hincapié en el anonimato que proporciona su servicio. Citando la página Ipredator.org (un servicio VPN iniciado por la gente detrás del proyecto Pirate Bay):

"Usted cambiará la dirección IP que recibe de su proveedor de Internet para obtener una dirección IP anónima. Usted obtiene una conexión segura/cifrada entre su computadora e Internet". (<https://www.ipredator.se>)

En efecto, cuando se accede a Internet a través de una conexión VPN parece como si la conexión se originara en la dirección IP de los servidores de IPredator.

# 20

## Publicaciones anónimas

Si usted es un activista que opera bajo un régimen totalitario, un empleado determinado a exponer algunas malas acciones de su empresa o un escritor vengativo que compone un retrato insidioso de su ex esposa, necesita proteger su identidad. Si no va a colaborar con los demás, debe enfocarse en el anonimato y no en el cifrado o la privacidad.

Si el mensaje es urgente y hay mucho en juego, una manera fácil es simplemente salir, ir a un lugar con Internet que no frecuente, crear una cuenta de correo electrónico específicamente para la ocasión, entregar los datos y descartar posteriormente esas cuentas. Si usted está en un apuro, considere usar MintEmail (<http://mintemail.com/>) o FilzMail (<http://www.filzmail.com/>), donde su cuenta expira a partir de 3 y 24 horas, respectivamente. No haga nada más mientras está allí, no marque su cuenta de gmail, no visite Facebook y borre toda la caché, los cookies y el historial y cierre el navegador web antes de salir.

Si sigue estas reglas básicas, lo peor que podría suceder - aunque altamente improbable - es que el equipo estuviera comprometido y registrara las pulsaciones del teclado, que revelarían las con-

traseñas o incluso la cara, en el caso de una cámara web conectada y operada remotamente. No haga esto en el trabajo o en un lugar donde usted sea un usuario registrado o visitante regular, como un club o una biblioteca.

Si desea mantener un flujo constante de comunicación e incluso establecer una conferencia, este método rápidamente se vuelve bastante engorrosos, y también podría quedarse sin cafés de Internet para usar. En este caso se puede usar una máquina de su propiedad, pero, si no se puede dedicarla especialmente a este fin, arranque la computadora con un sistema operativo diferente. Esto puede hacerse fácilmente mediante el uso de una memoria USB para arrancar un sistema operativo live por ejemplo TAILS (<https://tails.boum.org/>), el cual viene con TOR habilitado por defecto e incluye herramientas criptográficas actualizadas. En cualquier caso, use Tor para ocultar su IP.

Deshabilite todas las cookies, el historial y las opciones de caché y nunca utilice el mismo perfil o el mismo navegador para otras actividades. No sólo eso sería agregar datos a su topografía como usuario en la red, sino que también abre una ventana muy amplia para los errores. Si desea ayuda adicional, instale *Do Not Track Plus* y *Trackerblock* o *Ghosesty* en el menú de complementos de tu navegador.

Utilice contraseñas apropiadas y distintas para diferentes cuentas o incluso frases de paso (vea más sobre esto en la sección de consejos básicos). Proteja su sistema con una contraseña general, cámbiela a menudo y no la comparta con nadie, *especialmente* con su amante. Instale un capturador de teclado para ver si alguien se cuela en su correo electrónico, especialmente su amante. Configure sus preferencias generales para desconectarse de todos los servicios y las plataformas después de 5 minutos de inactividad. Mantenga su identidad de superhéroe en secreto.

Aunque usted pueda MANTENER tal nivel de disciplina, in-

---

cluso debe ser capaz de usar su propia conexión a Internet. Pero considere esto: no utilizar un sistema dedicado hace que sea muy difícil mantener todos los diferentes identidades separadas de forma segura, y la sensación de seguridad a menudo conduce a la falta de cuidado. Mantenga un nivel adecuado de neurosis.

Hoy en día existen muchas posibilidades de publicación, desde sitios de blogs sin costo (Blogspot, Tumblr, WordPress, Identica.ca) a PasteBins (ver glosario) y algunos contemplan específicamente a los usuarios anónimos como BlogACause. Global Voices Advocacy recomienda el uso de WordPress a través de la red Tor. Mantenga un nivel sano de escepticismo, todos tienen un interés comercial para que usted utilice estas plataformas “libres” y por lo tanto no puede confiar plenamente en ellas, especialmente en cuanto a que pueden estar sujeto a las demandas de una jurisdicción legal que no es la suya. Todos los proveedores son, cuando se llega a este punto, unos traidores.

Si el registro de estos servicios requiere una dirección de correo electrónico, cree una cuenta dedicada exclusivamente a este fin. Evite Gmail, Yahoo, Hotmail y otras grandes plataformas comerciales con antecedentes de entregar a sus usuarios y vaya a un servicio especializado como Hushmail (<https://www.hushmail.com/>). Para más información sobre correo electrónico anónimo, por favor, consulte el capítulo sobre Anonimato en la sección anterior.

## Distintos no

**No registre un dominio.** Existen servicios que protegen su identidad en una consulta simple acerca de quién es, como Anonymous Speech o Silent Register, pero tendrá que hacerlo mediante pago. A menos que tenga la posibilidad de comprar

uno en BitCoins, limítese a uno de los dominios ofrecidos por su plataforma de blogging tal como yourblogname.blogspot.com y elija una configuración fuera de su propio país. También, encuentre un nombre que no lo delate fácilmente. Si tiene problemas con esto, use un generador online de nombres de blogs.

**No abra una cuenta de red social asociada a su blog.** Si debe hacerlo, mantenga el nivel de higiene que mantiene para blogging y nunca jamás se conecte mientras usa su navegador habitual. Si tiene una vida en una red social pública, cuídese de tener todo junto. Tarde o temprano cometerá un error.

**No suba videos, fotos u archivos de audio** sin usar un editor que modifique o borre todos los metadatos (las fotos contienen información acerca de las coordenadas del lugar donde la fotografía fue tomada con cámaras digitales estándares, Smart-Phones, registradores y otros dispositivos añadidos por defecto. The *Metadata Anonymisation Toolkit* podría serle útil.

**No se olvide de las historias.** Añada X-Robots-Tag a sus encabezados http para detener a los robots de búsqueda que indexan su sitio web. Esto debería incluir repositorios como Wayback Machine de archive.org. Si no sabe qué es esto, busque a través de las líneas de “Robots Text File Generator”.

**No se olvide de los comentarios.** Si debe hacerlo, mantenga los niveles de higiene que usa para blogging y siempre cierre la sesión cuando haya terminado y por el amor de dios no se comporte como un troll. El infierno es agradable comparado con un blogger despreciado.

**No espere a lo último.** Si usted golpea la olla y se convierte en una sensación del blogging (como *Belle de Jour*, la estudiante británica de doctorado que se convirtió en una sensación y vendió un libro y reflexionó en dos programas de televisión acerca de su doble vida como prostituta de lujo) habrá una legión de periodistas, inspectores fiscales y fanáticos obsesivos

---

que escudriñen todos sus movimientos. Usted es solamente una persona: ellos la atraparán.

**No se detenga.** Si se da cuenta que ha cometido errores, aunque nadie lo haya atrapado, cierre todas sus cuentas, descubra las pistas y comience una identidad totalmente nueva. Internet tiene memoria infinita: un solo golpe y quedará fuera de combate.



# 21

## Correo electrónico anónimo

Cada paquete de datos que viaja a través de Internet contiene información acerca de su emisor y su destinatario. Esto se aplica al correo electrónico, así como a cualquier otra red de comunicación. Existen varias maneras de reducir la información de identificación pero no hay manera de eliminarla completamente.

### **Envío de mensajes por medio de cuentas de correo electrónico desechables**

Una opción es utilizar una cuenta de correo electrónico desechable. Se trata de una cuenta configurada en un servicio como Gmail o Hotmail, usada una vez o dos veces para el intercambio anónimo. Al registrarse en la cuenta, usted tendrá que proporcionar información falsa acerca de su nombre y ubicación. Después de usar la cuenta durante un corto periodo de tiempo, digamos 24 horas, nunca se debe volver a iniciar sesión. Si necesita comunicarse posteriormente, cree una nueva cuenta.

Es muy importante tener en cuenta que estos servicios llevan

un registro de las direcciones IP de dónde las utilizan. Si desea enviar información altamente sensible, usted tendrá que combinar el alta de una cuenta de correo electrónico con Tor para mantener su dirección IP oculta.

Si usted no está esperando una respuesta, un repetidor de correo anónimo como AnonEmail o Silentsender puede ser una solución útil. Un remailer es un servidor que recibe mensajes con instrucciones sobre dónde enviar los datos y actúa como intermediario, reenviándolo a partir de una dirección genérica sin revelar la identidad del remitente original. Esto funciona mejor cuando se combina con un proveedor de correo electrónico como Hushmail o Riseup que están especialmente configurados para conexiones seguras de correo electrónico.

Ambos métodos son útiles, pero sólo si usted recuerda siempre que el intermediario sabe de dónde viene el mensaje original y puede leerlos mensajes a medida que le llegan. A pesar de sus reclamos para proteger su identidad, estos servicios suelen tener acuerdos de usuario que indican su derecho “a divulgar a terceros ciertos datos de registro sobre usted” o si sospechan que pueden estar en peligro por los servicios secretos. La única forma de utilizar esta técnica en forma segura es no confiar en estos servicios plenamente, y aplicar medidas de seguridad adicionales: el envío a través de Tor utiliza una dirección de correo electrónico desecharable.

Si sólo necesita recibir correo electrónico, servicios como Mailinator MintEmail y darle una dirección de correo electrónico que se autodestruye después de unas pocas horas. Al registrarse en una cuenta, usted debe proporcionar información falsa acerca de su nombre y la ubicación y protegerse mediante el uso de Tor.

---

## **¡Sea cuidadoso con lo que dice!**

El contenido de su mensaje puede revelar su identidad. Si menciona detalles acerca de su vida, su geografía, relaciones sociales o apariencia social, las personas pueden ser capaces de determinar quién envió el mensaje. Cada palabra elegida y el estilo de escritura se pueden usar para descubrir quién está detrás de los mensajes anónimos.

No debe usar el mismo nombre de usuario para diferentes cuentas o un nombre que esté relacionado con usted tal como un apodo de su niñez o un personaje de su libro favorito. Nunca use una cuenta secreta para una comunicación personal habitual. Si alguien conoce sus secretos, no se comunique con esta persona usando esta dirección de correo electrónico. Si su vida depende de esto, cambie su cuenta secreta tan a menudo como le sea posible entre distintos proveedores.

Finalmente, una vez que tenga su cuenta de correo electrónico totalmente configurado para proteger su identidad, la vanidad es su peor enemigo. Debe evitar ser distinto. No trate de ser inteligente, extravagante o único. Incluso la forma de comenzar sus párrafos son datos valiosos para la identificación, especialmente en estos días en que cada ensayo de la escuela y la entrada del blog que ha escrito está disponible en la Internet. Poderosas organizaciones pueden efectivamente utilizar estos textos para construir una base de datos que pueda “rastrearlo digitalmente” por lo que ha escrito.

Correo electrónico anónimo

---

# 22

## Compartir archivos

El término *compartir archivos* se refiere a la práctica de compartir archivos en la red, a menudo con la distribución más amplia posible en mente. Desafortunadamente en los últimos años se ha asociado popularmente con la distribución de contenido registrado bajo ciertas licencias de derechos de autor que no permiten la distribución de copias (por ejemplo supuesta actividad criminal). A pesar de esta nueva asociación, el intercambio de archivos sigue siendo una herramienta vital para todo el mundo: desde grupos académicos a las redes científicas y las comunidades de software libre.

En este libro intentamos ayudarlo a que aprenda a distribuir archivos en forma privada, con el consentimiento de algunas personas, sin que otras puedan acceder al contenido que intercambia ni que la transacción sea interceptada. Usted está protegido por su derecho básico al anonimato y a no ser espiado. La sospecha de que los contenidos podrían haber sido robados y no ser suyos no es razón suficiente para socavar su derecho a la privacidad.

La historia de Internet está plagada de ataques de diferentes tipos de nodos de publicación y distribución, realizadas por

diferentes medios (orden judicial, ataques de denegación de servicio). Lo que este tipo de eventos han demostrado es que si uno quiere que la información esté disponible en forma persistente y resistente contra los ataques, es un error confiar en la neutralización de un único nodo.

Esto ha sido demostrado recientemente por la clausura del servicio de descarga directa Megaupload, cuya desaparición provocó la pérdida de grandes cantidades de datos de sus usuarios, en gran parte ajeno incluso a las supuestas infracciones de copyright que sirvieron de pretexto para su cierre. En la misma línea los ISPs suelen acabar con los sitios web que contengan material dudoso simplemente porque les resulta más barato hacerlo que acudir a los tribunales y que un juez decida. Estas políticas dejan la puerta abierta a la intimidación por parte de todo tipo de empresas, organizaciones e individuos listos y dispuestos a hacer un uso agresivo de cartas legales. Tanto los servicios de descarga directa como los ISP son ejemplos de estructuras centralizadas que no pueden ser invocados porque son puntos débiles para el ataque, y debido a que sus intereses comerciales no están alineados con los de sus usuarios.

Difundir a través de los archivos de distribución, la descentralización de los datos, es la mejor manera de defenderse contra estos ataques. En la siguiente sección dos ámbitos de intercambio de archivos se perfilan. El primero son las tecnologías estándar de p2p cuya técnica de diseño está determinado por la eficiencia de las redes para permitir la velocidad de distribución y descubrimiento de contenido a través de mecanismos de búsqueda asociados. El segundo se centra en I2P como un ejemplo de una darknet llamada, su diseño da prioridad a la seguridad y el anonimato durante otros criterios que ofrecen una robusta, aunque menos eficiente de los recursos, ruta de acceso a la disponibilidad persistente.

Los medios de compartir archivos mencionados a continuación

---

son sólo algunos ejemplos de las muchas tecnologías P2P que se han desarrollado desde 1999. BitTorrent y Soulseek tienen enfoques muy diferentes, sin embargo ambos fueron diseñados para la facilidad de uso por un público amplio y tienen importantes comunidades de usuarios. I2P, de más reciente desarrollo, tiene una base de usuarios pequeña.

**BitTorrent** se ha convertido en el sistema P2P para compartir archivos más popular. La controversia que lo rodea hoy en día irónicamente ha ayudado a la comunidad a crecer, mientras que la policía, impulsada por los poderosos dueños de los derechos de autor, aprovechan los registros de los servidores para perseguir a sus operadores, a veces hasta el punto de encarcelarlos como en el caso de The Pirate Bay.

**Soulseek** - si bien nunca ha sido la más popular entre las plataformas de intercambio de archivos, tampoco ese es su objetivo. Soulseek se centra en el intercambio de música entre los simpatizantes, productores independientes, aficionados e investigadores. El sistema y la comunidad que lo rodea está completamente aislada de la web: no hay enlaces externos a los archivos de Soulseek. Estos archivos se mantienen exclusivamente en los discos duros de sus usuarios. El contenido de la red depende totalmente de cuántos miembros están conectados y cuántos lo comparten. Los archivos se transfieren sólo entre dos usuarios a la vez y nadie más que esos dos usuarios se involucran. Debido a esta “introvertido” carácter - y la especificidad de su contenido - Soulseek se ha mantenido fuera de la vista de los defensores de los derechos de autor y la legislación anticopia.

**I2P** es uno de varios sistemas desarrollados para resistir la censura (otros incluyen FreeNet y Tor) y cuenta con una comunidad de usuarios mucho menor, se destaca aquí por su inclusión de la funcionalidad de Bit Torrent en su instalación básica. Estos sistemas también pueden ser utilizados para proporcionar servicios ocultos, entre otros, lo que le permite publicar páginas

Web en sus entornos..

## BitTorrent

BitTorrent es protocolo P2P que facilita la distribución de los datos almacenados en varios nodos / participantes de la red. No hay servidores centrales o concentradores, cada nodo es capaz de intercambiar datos con cualquier otro nodo, a veces cientos de ellos al mismo tiempo. El hecho de que los datos se intercambian en partes entre numerosos nodos permite grandes velocidades de descarga de los contenidos más populares en las redes BitTorrent, por lo que se ha convertido rápidamente en el estándar de facto entre las plataformas de intercambio de archivos P2P.

Si utiliza BitTorrent para distribuir material de dudosa legalidad, usted debe saber que las fuerzas de seguridad habitualmente recopilan información sobre presuntos infractores participando en enjambres torrent, observando y documentando el comportamiento de los otros pares. El gran número de usuarios en constante aumento crea un problema para aplicar este sistema - simplemente no tienen recursos suficientes para perseguir a todos los usuarios. Cualquier caso judicial requerirá evidencia real de transferencia de datos entre el cliente y otro par (y por lo general la evidencia de la carga del archivo); sin embargo, es suficiente que usted proporciona una parte del archivo, no el archivo en su totalidad, para ser acusado. Si usted prefiere ser mas precavido, debe utilizar una VPN para enrutar el tráfico de BitTorrent, como se detalla en el capítulo **Uso de VPN**.

La descarga de un archivo de la red BitTorrent comienza con un archivo torrent o con un enlace magnet. Un archivo torrent es un archivo pequeño que contiene información sobre los archivos de mayor tamaño que desea descargar. El archivo torrent le dice

---

a su cliente de torrent los nombres de los archivos que se comparten, una dirección URL para el seguidor y un código hash, que es un código único derivado del archivo subyacente al cual representa - algo así como una identificación o número de catálogo. El cliente puede utilizar el hash para encontrar la semillas de otros (para subir) esos archivos, así puede descargar desde su computadora y comprobar la autenticidad de los fragmentos a medida que llegan.

Un *enlace magnet* elimina la necesidad de un archivo torrent y es esencialmente un hipervínculo que contiene una descripción de ese torrent que su cliente puede usar inmediatamente para empezar a buscar personas que comparten el fichero que está dispuesto a descargar. Los enlaces magnet no requieren de un tracker, sino que dependen de la *tabla hash distribuidas (DHT)* - se puede leer más en el Glosario – y en *Mecanismo de intercambio*. Los enlaces magnet no hacen referencia a un archivo por su ubicación (por ejemplo, mediante las direcciones IP de las personas que tienen el archivo o URL) sino que definen los parámetros de búsqueda que permiten encontrar el archivo. Cuando se carga un enlace magnet, el cliente torrent inicia una búsqueda de disponibilidad que se transmite a otros nodos y es básicamente una nota - “¿quién tiene algo que coincide con el hash?”. El cliente torrent se conecta a los nodos que respondieron a la nota de salida y comienza a descargar el archivo.

BitTorrent utiliza cifrado para evitar que los proveedores y otros man-in-the-middle bloqueen o espíen el tráfico basándose en el contenido que usted intercambia. Ya que los enjambres de BitTorrent (rebaños de semillas y leechers) son libres para que todo el mundo pueda unirse a ellos es posible que alguien lo haga y recopile información acerca de todos los pares conectados. El uso de enlaces magnet no evitara que lo detecten entre la multitud, ya que todos los nodos que comparten el mismo archivo deben comunicarse entre sí -y, por tanto, aunque sólo uno de los nodos

del enjambre sea un trámposo, será capaz de ver su dirección IP. También será capaz de determinar si usted está sembrando los datos mediante el envío de su nodo de una solicitud de descarga.

Un aspecto importante del uso de BitTorrent es digno de una mención especial. Cada fragmento de datos que recibe (leecher) está siendo compartida instantáneamente (sin semillas) con otros usuarios de BitTorrent. Por lo tanto, un proceso de descarga se transforma en un proceso (involuntario) de publicación, utilizando un término legal pone a disposición los datos, antes de que la descarga se complete. Mientras BitTorrent se utiliza a menudo para volver a distribuir el software libremente disponible y legítimo, películas, música y otros materiales, su capacidad de “puesta a disposición” ha creado mucha controversia y dio lugar a un sinfín de batallas legales entre los titulares de derechos de autor y los facilitadores de plataformas BitTorrent. En el momento de escribir este texto, el co-fundador de The Pirate Bay Gottfrid Svartholm se encuentra detenido por la policía sueca tras una orden internacional dictada contra él.

Por estas razones, y por las campañas de relaciones públicas de los titulares de los derechos de autor, el uso de las plataformas de BitTorrent se ha convertido prácticamente en sinónimo de piratería. Y aunque todavía no está claro el significado de términos como piratería, derechos de autor y propiedad en el contexto digital, muchos usuarios comunes de BitTorrent han sido perseguidos acusados de violar las leyes de derechos de autor.

La mayoría de los clientes torrent le permiten bloquear direcciones IP de los trolls conocidos de derechos de autor usando listas negras. En lugar de usar torrents públicos también se puede unir a trackers de BitTorrent cerrados o utilizarlos a través de VPN o Tor.

En las situaciones en las que usted cree que debería estar pre-

---

ocupado por el tráfico de BitTorrent y su anonimato debería verificar lo siguiente:

- Compruebe si su cliente soporta listas negras de pares.
- Compruebe si las definiciones de las listas negras de pares se actualizan diariamente.
- Asegúrese que su cliente soporte la totalidad de los protocolos más recientes - DHT, PEX y enlaces Magnet.
- Elija un cliente torrent que soporte cifrado de pares y habilítelo.
- Actualice o cambie su cliente torrent si algo de lo mencionado más arriba no está disponible.
- Use una conexión VPN para ocultarle su tráfico BitTorrent a su ISP. Asegúrese que su proveedor de VPN permite el tráfico P2P. Vea más consejos y recomendaciones en el capítulo Uso de VPN.
- No siembre ni guarde semillas si no sabe mucho acerca de ello.
- Sospeche de los enlaces muy populares o con comentarios muy positivos.
- Verifique si su cliente torrent soporta listas negras de pares.

## SoulSeek

Como en el caso de los programas para compartir archivos entre pares (P2P), los usuarios de Soulseek determinan el contenido disponible, y cuáles archivos se pueden compartir. La red tuvo históricamente una mezcla de música diversa, incluyendo artistas independientes y alternativos, música inédita, tales como demos y cintas de las mezclas, grabaciones piratas, etc. Está totalmente financiado por donaciones, sin publicidad ni cobro de tarifas a usuarios.

Soulseek no avala ni aprueba el intercambio de materiales con copyright. Sólo debe compartir y descargar archivos para los cuales usted está legalmente autorizado, o ha recibido permiso.” (consulte su página web)

La red de Soulseek depende de un par de servidores centrales. Uno soporta al cliente original y a la red, y el otro soporta a la red más nueva. Mientras que estos servidores centrales son claves para coordinar búsquedas y hospedar salas de chat, no juegan ningún rol en la transferencia de archivos entre usuarios, que se desarrolla directamente entre ellos.

Los usuarios pueden buscar por ítem, los resultados devueltos serán una lista de los archivos cuyos nombres coinciden con el término de búsqueda utilizado. Las búsquedas pueden ser explícitas o pueden utilizar comodines/patrones o condiciones para ser excluidos. Una característica específica al motor de búsqueda Soulseek es la inclusión de los nombres de las carpetas y las rutas de archivo en la lista de búsqueda. Esto permite a los usuarios buscar por nombre de carpeta.

La lista de resultados de búsqueda muestra los detalles, como el nombre completo y la ruta del archivo, su tamaño, el usuario que aloja el archivo, junto con la tasa promedio de transferencia de los usuarios y, en el caso de archivos mp3, detalles breves acerca de la pista codificada en sí, tales como la velocidad de bits, longitud, etc. La lista de búsqueda resultante puede entonces ser ordenada en una variedad de formas y archivos individuales (o carpetas) seleccionados para su descarga.

A diferencia de BitTorrent, Soulseek no es compatible con la descarga desde fuentes múltiples o “swarming” como otros clientes post-Napster, y deben buscar un archivo solicitado desde una sola fuente.

Si bien el software Soulseek es libre, existe un sistema de

---

donación para apoyar el esfuerzo de programación y el costo de mantenimiento de los servidores. A cambio de donaciones, a los usuarios se les concede el privilegio de ser estar por delante de los usuarios que no hagan donaciones en una cola de descarga de archivos (pero sólo si los archivos no se comparten en una red de área local). Los algoritmos del protocolo de búsqueda Soulseek no se publican, ya que esos algoritmos se ejecutan en el servidor. Sin embargo, existen muchas implementaciones libres de software para clientes y servidores en GNU/Linux, OS X y Windows.

En cuanto a los temas de privacidad y copyright Soulseek está bastante lejos de BitTorrent también. Soulseek ha sido llevado ante los tribunales sólo una vez, en 2008, pero incluso eso no iba a ninguna parte. No hay indicios de usuarios Soulseek que hayan sido llevados ante la corte o acusados de distribución ilegal de material con copyright u otros crímenes del ‘milenio digital’.

Si desea usar la red Soulseek con algún grado de anonimato, deberá usarla sobre una VPN.

## I2P

I2P comenzó como una ramificación del proyecto Freenet, originalmente concebida como un método de publicación y distribución resistente a la censura. Desde su sitio web:

El proyecto I2P se formó en el 2003 para apoyar los esfuerzos de aquellos que tratan de construir una sociedad más libre, ofreciéndoles un sistema de comunicación incensurable, anónimo y seguro. I2P es un esfuerzo de desarrollo que produce una red de baja latencia, totalmente distribuida, autónoma, escalable, anónima y resistente. El objetivo es op-

erar con éxito en entornos hostiles - incluso cuando una organización con recursos financieros o políticos lo ataca. Todos los aspectos de la red son de código abierto y están disponibles sin costo, ya que debe asegurar a las personas que lo usan que el software hace lo que dice, al igual que permite que otros puedan contribuir y mejorarlo para derrotar los intentos agresivos que quieren sofocar la libertad de expresión. (<http://www.i2p2.de/>)

Para una guía de instalación del software y la configuración de su navegador web consulte la sección sobre Intercambio seguro de archivos - Instalación de I2P. Una vez terminado, el lanzamiento lo llevará a una página de la consola que contiene enlaces a otros sitios y servicios populares. Además de las páginas web habituales (conocidas como eePsites) hay una amplia gama de servicios de aplicaciones disponibles desde la herramienta de blogging para Syndie construido en un cliente de BitTorrent que funciona a través de una interfaz web.

# 23

## Llamadas seguras

Las llamadas telefónicas hechas a través del sistema normal de telecomunicaciones tienen algunas formas de protección contra la intercepción de terceros, por ejemplo, los teléfonos móviles GSM cifran las llamadas. Sin embargo, no están cifradas de extremo a extremo, y los proveedores de telefonía están cada vez más obligados a dar a los gobiernos y a las instituciones de la ley acceso a sus llamadas. Además, el cifrado utilizado en GSM se ha roto y cualquier persona con interés y un capital suficiente puede comprar el equipo para interceptar llamadas. Un interceptor GSM (<http://en.interceptor.ws/catalog/2087.html>) es un dispositivo disponible para la plataforma para grabar conversaciones de teléfono móvil cuando se encuentra en las proximidades de la llamada. Los sistemas centralizados o propietarios como Skype también cifran las llamadas, pero están construidos con puertas traseras para que accedan los servicios secretos y los gobiernos con conocimiento de sus propietarios (en el caso de Skype, Microsoft). Adicionalmente, existe una amplia clasificación de dispositivos llamados receptores IMSI los cuales pueden recolectar más información acerca de los teléfonos móviles, incluso el contenido de su comunicación.

Sin embargo, existen varias herramientas que usted puede utilizar para asegurar su teléfono usando cifrado punto a punto.

## iOS - Instalando Signal

Los creadores de TextSecure proporcionan una herramienta FLOSS llamada Signal. (<https://itunes.apple.com/us/app/signal-private-messenger/id874139669?mt=8>) Signal usa métodos de cifrado similares a SilentCircle pero provee su servicio con herramientas FLOSS. Además, su GUI (interfaz gráfica de usuario) es extremadamente fácil de usar. Signal detectará en forma transparente si usted está hablando con un usuario de Signal y le preguntará si desea establecer una “llamada segura” (con Signal) o una “llamada insegura” (sin cifrado punto a punto).

## Android - Instalando RedPhone

También de los creadores de Signal, existe una herramienta FLOSS llamada RedPhone. <https://play.google.com/store/apps/details?id=org.th0UGHT0LUTIONS.RDPhN&hl=es> Nuevamente, RedPhone usa métodos de cifrado similares a SilentCircle pero provee sus servicios usando herramientas FLOSS. También en este caso, su GUI detectará en forma transparente si usted está hablando con otros usuarios de Signal o RedPhone y le preguntará si desea establecer una “llamada segura” (con RedPhone) o una “llamada insegura” (sin cifrado punto a punto). Desafortunadamente, RedPhone requiere el framework de Google Play sino no trabajará en dichos teléfonos (Cyanogenmod u otras ROMs similares). Mensajería segura  
=====

Los SMS son mensajes cortos enviados entre teléfonos móviles.

---

El texto se envía sin cifrar y pueden ser leídos y almacenados por los proveedores de telefonía móvil y otras partes que tienen acceso a la infraestructura de la red a la que está conectado. Para evitar que sus mensajes sean interceptados usted tiene que utilizar cifrado punto a punto en sus mensajes de texto.

## Android

- **TextSecure** - WhisperSystems provee un sistema de cifrado de SMS para Android llamado TextSecure, basado en la criptografía de clave pública que asegura que los mensajes se cifren desde la conexión y que también se almacenen en una base de datos cifrada en el dispositivo, sin embargo, para asegurar el cifrado de la conexión, ambas partes deben usar la aplicación, Es Open Source y está disponible a través de PlayStore

La tecnología detrás del cifrado (llamada //axolotl//) extiende el protocolo OTR para que el mensaje pueda ser cifrado y enviado aunque no estén online todas las partes intervinientes en la comunicación.



# 24

## Usando Thunderbird



Figure 24.1: Thunderbird

En las secciones siguientes vamos a usar el programa de correo electrónico Thunderbird de Mozilla para mostrarle cómo configurar su cliente para mayor seguridad. Al igual que el navegador Mozilla Firefox, Thunderbird tiene muchas ventajas sobre sus contrapartes de seguridad como Apple Mail y Outlook.

Thunderbird es un “agente de usuario de correo” (MUA). Esto es diferente de web basadas en servicios de correo electrónico como Gmail de Google. Usted debe instalar la aplicación Thunderbird en el equipo. Thunderbird tiene una interfaz agradable y las características que le permiten gestionar varios buzones, organizar los mensajes en carpetas, y la búsqueda a través de correos con facilidad.

Thunderbird puede ser configurado para trabajar con su actual cuenta de correo electrónico, ya sea un proveedor de servicios de

Internet (como Comcast) o un proveedor de correo electrónico basado en la web (como Gmail).

Thunderbird presenta muchas ventajas sobre las interfaces web de correo electrónico. Estas serán discutidos en el capítulo siguiente. La más importante es que Thunderbird permite mucho mayor privacidad y seguridad.

Esta sección proporciona información sobre cómo instalar Thunderbird en Windows, Mac OS X y Ubuntu.

## Instalación de Thunderbird en Windows

La instalación de Thunderbird involucra dos pasos: primero, descargar el software y luego ejecutar el programa de instalación.

1. Visite la página de descarga de Thunderbird <http://www.mozilla.org/en-US/thunderbird/>. Esta página detectará el sistema operativo de su computadora y el idioma, recomendándole la mejor versión disponible para su uso.

Si desea usar Thunderbird en un idioma y/o sistema operativo diferente, pulse *Other Systems and Languages* en el lado derecho de la página y elija la versión de su agrado.

2. Haga click en el botón de descarga para grabar el programa de instalación en su computadora.

Pulse el botón **Save** para grabar el archivo de configuración de Thunderbird en su computadora.

3. Cierre todas las aplicaciones en uso.
4. Busque el archivo de configuración (generalmente está en su carpeta de descargas o en el escritorio) y haga doble



Figure 24.2: Instalación de Thunderbird

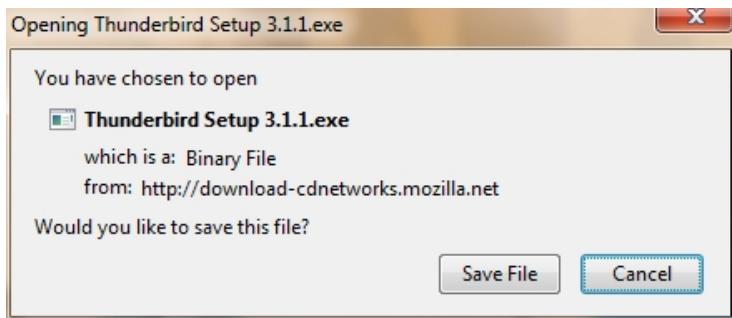


Figure 24.3: Descarga de Thunderbird

click para iniciar la instalación. La primer cosa que el instalador hará será mostrarle en pantalla la bienvenida del asistente de configuración **Welcome to the Mozilla Thunderbird Setup Wizard**.



Figure 24.4: Comenzando la instalación de Thunderbird

Pulse el botón **Next** para comenzar la instalación. Si desea detenerla, haga click en el botón **Cancel**.

5. Lo próximo que verá es la pantalla de tipo de configuración, **Setup Type**. Para la mayoría de los usuarios la opción estándar es buena aunque no suficiente para todas sus necesidades. La opción de configuración personalizada se recomienda exclusivamente para usuarios con experiencia. Note que Thunderbird se instalará él mismo como su aplicación de correo por defecto. Si no desea

---

que esto ocurra, desmarque la casilla de verificación etiquetada como **Use Thunderbird as my default mail application**.

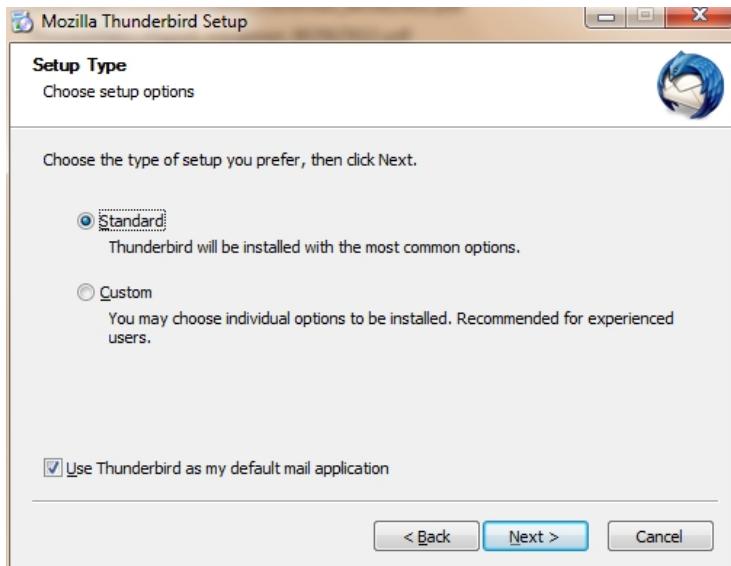


Figure 24.5: Configuración

Pulse el botón **Next** para continuar con la instalación.

6. Después que Thunderbird ha sido instalado, pulse el botón **Finish** para cerrar el asistente de configuración.

Si marca la opción **Launch Mozilla Thunderbird** en la casilla de verificación, Thunderbird iniciará después de haber sido instalado.

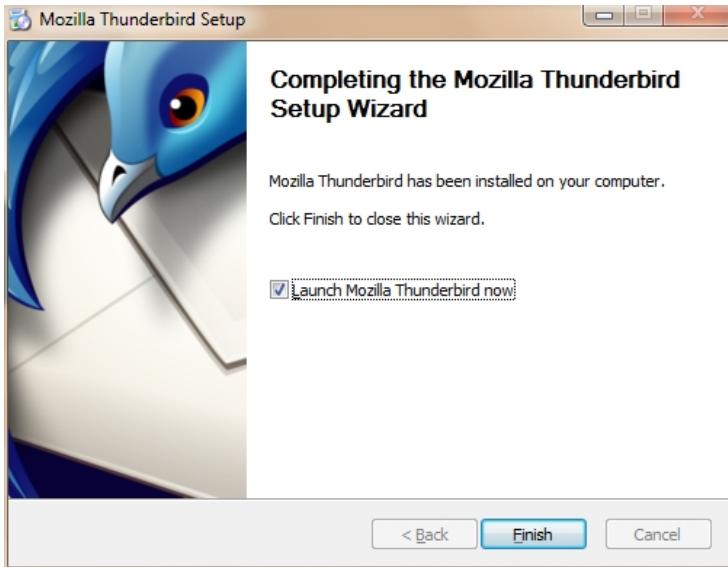


Figure 24.6: Finalizando la instalación

---

## Instalación de Thunderbird en Ubuntu

Existen dos procedimientos de instalación diferentes según la versión de Ubuntu: uno para la versión 10.04 o posterior, y otra para las anteriores. Describiremos ambas más abajo.

Thunderbird no se ejecutará sin las siguientes librerías o paquetes instalados en su computadora:

- GTK+ 2.10 o superior
- GLib 2.12 o superior
- Pango 1.14 o superior
- X.Org 1.0 o superior

Mozilla recomienda que un sistema GNU/Linux tenga también las siguientes librerías o paquetes:

- NetworkManager 0.7 o superior
- DBus 1.0 o superior
- HAL 0.5.8 o superior
- GNOME 2.16 o superior

## Instalación de Thunderbird en Ubuntu 12.04 o posteriores

Si está usando 12.04 o una versión posterior, la manera más sencilla de instalar Thunderbird es mediante el Ubuntu Software Center.

1. Tipee Software en la ventana de búsqueda Unity.
2. Haga click en ‘Ubuntu Software Center’
3. Tipee “Thunderbird” en la caja de búsqueda y pulse Enter en su teclado. El Ubuntu Software Center encontrará a Thunderbird en su lista de software disponible.



Figure 24.7: Buscando Thunderbird

4. Haga click en el botón **Install**. Si Thunderbird necesita alguna librería adicional, el Ubuntu Software Center le avisará y lo instalará junto con Thunderbird.

Usted puede encontrar el acceso directo a Thunderbird en las opciones de Internet dentro del menú de aplicaciones:

## Instalación de Thunderbird en Mac OS X

Para instalar Thunderbird en su Mac, siga los siguientes pasos:

1. Vaya a la página de descargas de Thunderbird <http://www.mozilla.org/en-US/thunderbird/>. Esta página detectará el sistema operativo de su computadora y el idioma, recomendándole la mejor versión disponible para su uso.
2. Descargue la imagen de disco Thunderbird. Cuando complete la descarga, la imagen de disco se abrirá automáticamente y se montará un nuevo volumen denominado *Thunderbird*.

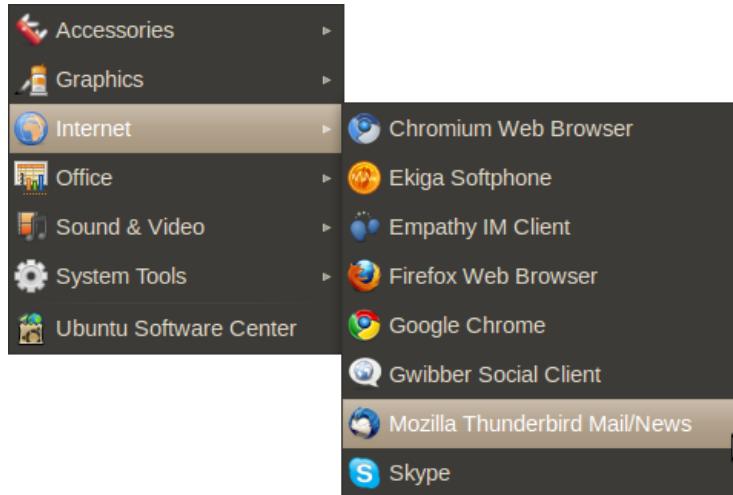


Figure 24.8: Menú de aplicaciones



Figure 24.9: Instalación de Thunderbird

Si el volumen no se monta automáticamente, abra la carpeta de descargas y haga doble click en la imagen del disco para montarla. Aparecerá una ventana de localización:



Figure 24.10: Abriendo la imagen

3. Arrastre el ícono de Thunderbird dentro de su carpeta de aplicaciones. ¡Thunderbird ya está instalado!
4. Opcionalmente, arrastre el ícono de Thunderbird desde la carpeta de aplicaciones dentro del Dock. Seleccionar el ícono de Thunderbird desde el Dock le permitirá abrirlo rápidamente.

**Nota:** Cuando ejecute Thunderbird por primera vez, las versiones más recientes de Mac OS X (10.5 o posterior) le avisarán que la aplicación Thunderbird.app fue descargada desde Inter-



Figure 24.11: Abriendo Thunderbird

net.

Si descargó Thunderbird desde el sitio web de Mozilla, haga click en el botón **Open**.



Figure 24.12: Abriendo Thunderbird

## Usando Thunderbird por primera vez

Al usar Thunderbird por primera vez será guiado a través de la configuración de su cuenta de correo electrónico. Estos parámetros son definidos por su proveedor de correo electrónico (su ISP o su proveedor de servicios de correo electrónico basado en la web). El próximo capítulo describe cómo configurar su cuenta con la máxima seguridad.

# 25

## Configuración de cuentas seguras

Existe una manera correcta (segura) de configurar su conexión con los servidores de correo electrónico de su proveedor y una manera incorrecta (insegura). El aspecto más importante de la seguridad en los correos electrónicos es el tipo de conexión que establecerá con el servidor de su proveedor.

Siempre que sea posible, debería conectarse usando los protocolos **SSL** (Secure Socket Layer) y **TLS** (Transport Layer Security). (**STARTTLS**, otra versión disponible cuando configura una cuenta, es una variación de SSL/TLS.) Estos protocolos impiden que su propio sistema (más allá de Thunderbird) y todos los puntos entre sus sistema y el servidor de correo puedan ser interceptados y robadas sus contraseñas. Además, también impiden que los la lectura del contenido de sus mensajes.

Estos protocolos, sin embargo, sólo aseguran la conexión entre el ordenador y el servidor de correo. No protegen el canal de información en todo el camino hasta el destinatario del mensaje. Una vez que los servidores de correo reenvían el mensaje para la entrega, el mensaje puede ser interceptado y leído por los puntos intermedios entre el servidor de correo y el destinatario.

Aquí es donde **PGP** (Pretty Good Privacy) entra, lo cual se describe en el capítulo siguiente.

El primer paso para asegurar al correo electrónico es tener una conexión segura entre su sistema y los servidores de correo. En este capítulo se describe cómo configurar su cuenta de correo electrónico de la manera correcta.

## Requisitos de configuración

Al configurar una cuenta, Thunderbird intenta determinar los parámetros de conexión (de la cuenta de correo electrónico y los datos de la cuenta que usted proporciona) con su proveedor de correo electrónico. Aunque Thunderbird conoce los parámetros de conexión para muchos proveedores de correo electrónico, no los conoce a todos. Si los parámetros no son conocidos por Thunderbird, usted tendrá que proporcionar la siguiente información para configurar su cuenta:

- **Su nombre de usuario**
- **Su contraseña**
- **Servidor entrante:** nombre (como `imap.example.com`), protocolo (POP o IMAP), el puerto (por defecto, 110), y el protocolo de seguridad
- **Servidor saliente:** nombre (como `smtp.example.com`), el puerto (por defecto, 25), y el protocolo de seguridad

Debería haber recibido esta información de su proveedor de hosting. Alternativamente, usted puede encontrar esta información en las páginas de soporte en el sitio Web de su proveedor de hosting. En nuestro ejemplo vamos a utilizar la configuración del servidor de Gmail. Puede utilizar Thunderbird con su cuenta de Gmail. Para ello, es necesario cambiar una opción de configuración de su cuenta. Si no está usando una cuenta de Gmail, saltee la siguiente sección.

---

## Preparación de una cuenta de Gmail para usar con Thunderbird

Accede a tu cuenta de Gmail en tu navegador. Selecciona **Configuración** de opciones en la parte superior derecha, luego vaya a la pestaña **Forwarding and POP/IMAP**. Pulse **Enable IMAP** y luego **Save Changes**.



Figure 25.1: Habilitación de IMAP en Gmail

## Configurar Thunderbird para usar SSL / TLS

Al iniciar Thunderbird por primera vez, se entra en un proceso de configuración paso a paso para configurar su primera cuenta. (Se puede invocar la interfaz de configuración de la cuenta en cualquier momento seleccionando **File | New | Mail Account**). En la primera pantalla, se le pedirá su nombre, su dirección de correo electrónico y su contraseña. El valor que introduzca por nombre no tiene por qué ser su nombre real. Se

muestra al destinatario de sus mensajes. Introduzca la información y haga click en **Continue**.

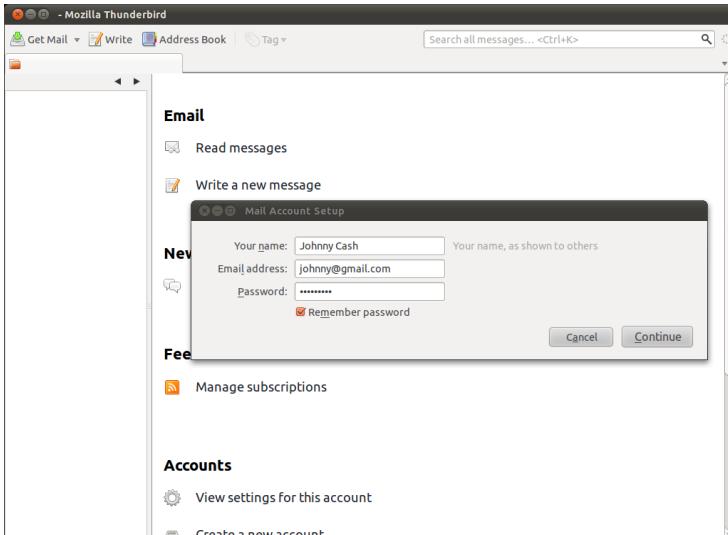


Figure 25.2: Configurando Thunderbird

En la siguiente pantalla, Thunderbird intentará determinar los nombres de los servidores basados en su dirección de correo electrónico. Esto puede llevar algún tiempo, y sólo funcionará si Thunderbird sabe la configuración de los servidores de tu proveedor. En cualquier caso, se le presentará una ventana donde se puede modificar la configuración. En el siguiente ejemplo, Thunderbird ha detectado la configuración de forma automática. Usted puede ver el protocolo en la parte derecha de los nombres de servidor. Esto debe ser tanto **SSL/TLS** o **STARTTLS**. *De lo contrario su conexión es insegura y usted debe tratar de configurarla manualmente.*

Cuando haya terminado, haga click en **Create account**. Si

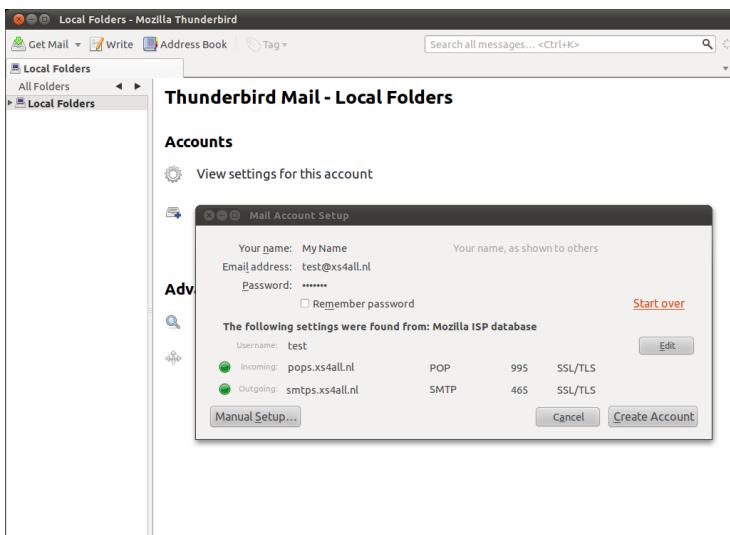


Figure 25.3: Configurando las cuentas

Thunderbird no pudo determinar la configuración del servidor, haga click en **Manual setup** para configurar los nombres de servidor usted mismo.

## Configuración manual

Utilice la interfaz para configurar manualmente las cuentas en Thunderbird. El cuadro de diálogo de configuración de la cuenta se abrirá automáticamente si se selecciona **Manual setup** en el asistente de configuración. En este caso, sólo estamos interesados en los nombres de servidores de correo entrante y saliente, y el protocolo que se utiliza para conectarse con ellos. Como se puede ver en los ejemplos siguientes, ingresamos los nombres de los servidores de Gmail y los forzamos a utilizar **TLS/SSL**, un método seguro para conectarse a los servidores.

En ‘Configuración del servidor’, encontraremos sólo el servidor entrante (**IMAP**) y la configuración de esa cuenta específica.

Bajo **Server Name** introduzca el nombre del servidor IMAP, en este caso **mail.gmail.com**.

*Como usted puede ver, hemos seleccionado ‘SSL/TLS’ en la configuración de seguridad de conexión. o fuerza el cifrado. No te asustes por el método de autenticación **contraseña normal**. La contraseña se cifra automáticamente debido a nuestras conexiones seguras al servidor.*

Por último, configure el servidor de correo saliente para la cuenta. Haga click en **Outgoing Server (SMTP)** en el panel izquierdo.

Una vez más, hemos seleccionado **SSL/TLS** en **Connection security**. El puerto por defecto será 465 y generalmente no debería ser cambiado.

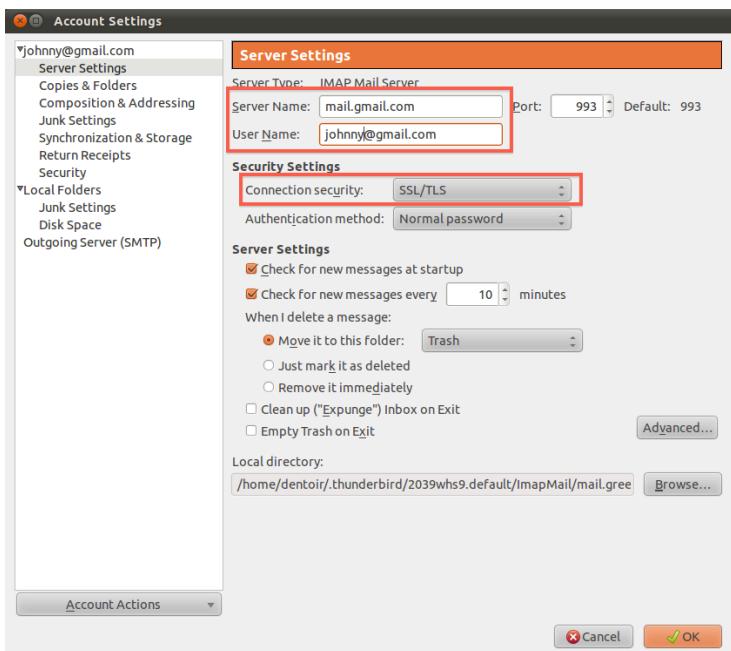


Figure 25.4: Configurando la seguridad

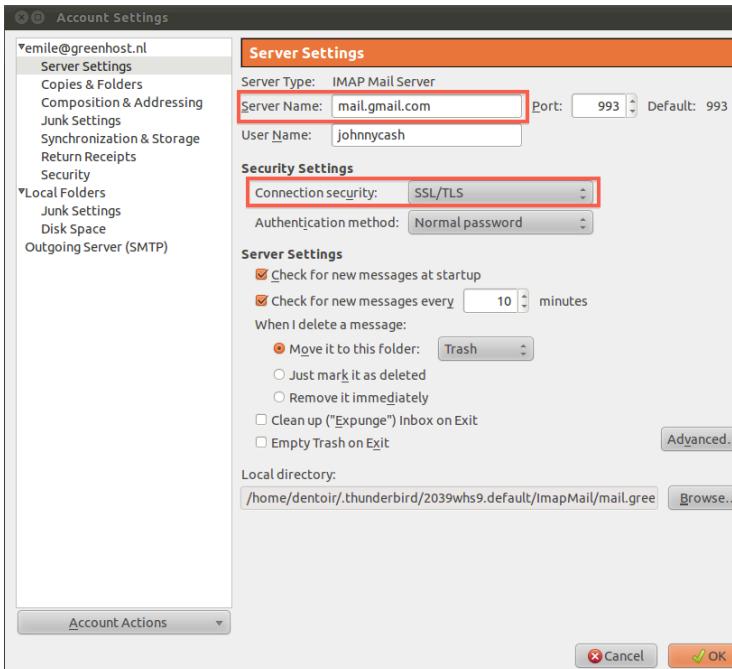


Figure 25.5: Configuración de correo entrante

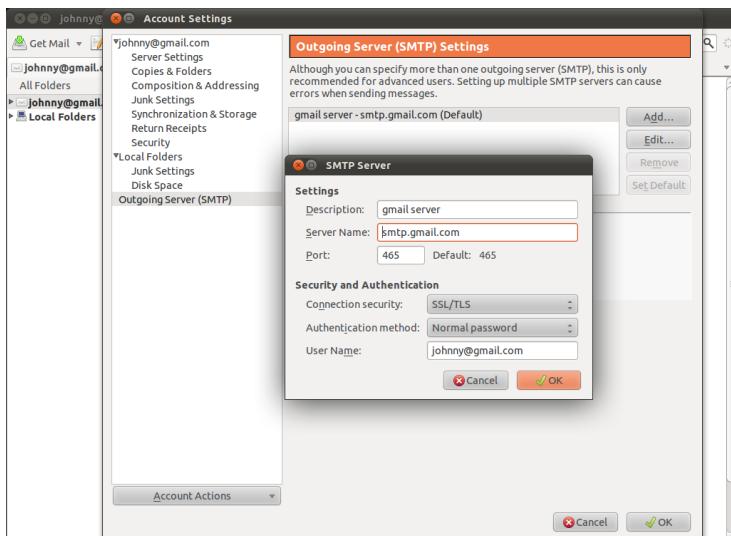


Figure 25.6: Configuración de correo saliente

## Finalizando la configuración, diferentes métodos de cifrado

Pruebe la configuración de Thunderbird intentando enviar y recibir mensajes. Algunos proveedores de almacenamiento de correo electrónico no soportan el protocolo SSL/TLS, la opción favorita. Debería aparecer un mensaje de error diciendo que el protocolo de autenticación no está soportado por el servidor. Entonces, pruebe a utilizar STARTTLS. En las dos pantallas de más abajo, seleccione “STARTTLS” en “Connection security”. Si este método también falla, póngase en contacto con su proveedor de almacenamiento de correo electrónico y pregúntele ellos ofrecen otra manera de conectarse de forma segura a sus servidores. Si no le permiten hacerlo entonces usted debe quejarse y considerar seriamente la posibilidad de cambiar a un proveedor diferente.

## De regreso a las pantallas de configuración

En cualquier momento usted puede reconfigurar sus cuentas de correo yendo a la barra de menú de Thunderbird y pulsando **Edit | Account Settings** (GNU/Linux), **Tools | Account Settings** (Windows y Mac OS X).

# 26

## Parámetros adicionales de seguridad

Thunderbird provee medidas de seguridad adicional para protegerlo del correo basura, robo de identidad, virus (con la ayuda de su software antivirus, por supuesto), robo de propiedad intelectual, y sitios web maliciosos.

Veremos las siguientes características de seguridad de Thunderbird. Primero un poco de historia sobre por qué debe tener en cuenta algunas de estas medidas:

- **Controles de correo basura adaptables.** Le permiten entrenar a Thunderbird para que pueda identificar correo electrónico no deseado (SPAM) y eliminarlo de su bandeja de entrada. También puede marcar los mensajes como correo basura manualmente si el sistema de su proveedor de correo electrónico falla el correo basura y lo deja pasar.
- **Integración con el software anti-virus.** Si su software antivirus es compatible con Thunderbird, puede utilizarlo para poner en cuarentena a los mensajes que contienen virus u otros contenidos maliciosos. Si usted se pregunta qué software antivirus trabaja con Thunderbird,

puede encontrar una lista aquí: [http://kb.mozilla.org/Antivirus\\_software](http://kb.mozilla.org/Antivirus_software).

- **Contraseña maestra.** Para su conveniencia, usted puede hacer que Thunderbird recuerde cada una de las contraseñas individuales de sus cuentas de correo electrónico. Puede especificar una contraseña maestra que se introduzca cada vez que inicie Thunderbird. Esto le permitirá a Thunderbird abrir todas tus cuentas de correo electrónico con sus contraseñas guardadas.
- **Restricciones a las cookies.** Algunos blogs y sitios web intentan enviar cookies (una pieza de código que almacena información de los sitios web en su computadora) con sus feeds RSS. Estas cookies son utilizadas con frecuencia por los proveedores de contenido para ofrecer publicidad dirigida. Thunderbird rechaza las cookies de forma predeterminada, pero se puede configurar para aceptar algunas o todas las cookies.

En la caja de diálogo Options/Preferences de la sección Security Preferences puede establecer las preferencias para estas funciones.

- En Windows y Mac OS X, vaya al menú ‘Herramientas’ y haga clic en ‘Opciones’.
- En Ubuntu u otras versiones de Linux, vaya al menú ‘Editar’ y haga clic en ‘Preferencias’.

## Configuración de correo basura

1. En la caja de diálogo de Preferences/Options, pulse ‘Security’ y luego seleccione la pestaña ‘Junk’.
2. Haga lo siguiente:
  - Dígale a Thunderbird que maneje los mensajes marcados como basura, seleccionando la casilla de veri-

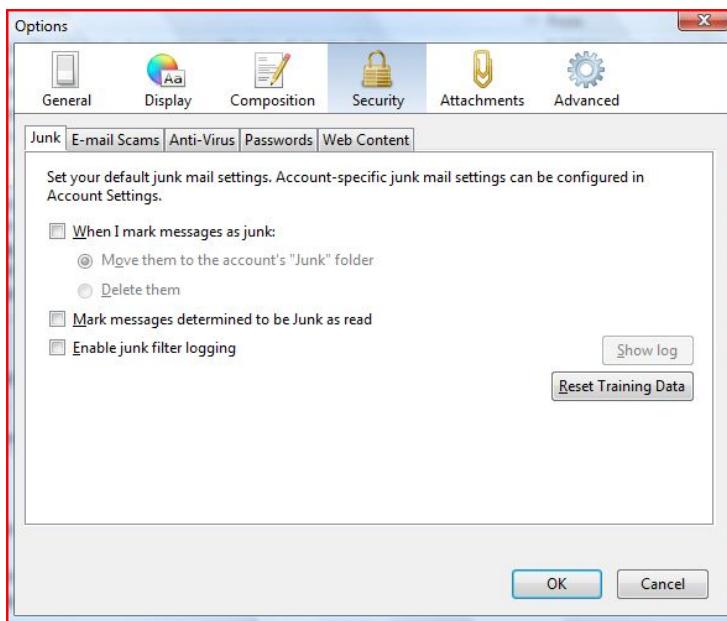


Figure 26.1: Seguridad en Thunderbird

- ficación etiquetada como ‘When I mark message as junk’.
- Para que Thunderbird mueva estos mensajes a la carpeta de correo basura, seleccione el botón de opción ‘Move them to account’s ‘Junk’ folder’.
  - Para que Thunderbird borre el correo basura recibido, seleccione el botón de inicio ‘Delete them’.
3. Thunderbird marcará los correos basura como leídos si usted selecciona la casilla de verificación etiquetada ‘Mark messages determined to be Junk as read’.
  4. Si desea mantener un registro de correo basura recibido, seleccione la casilla de verificación ‘Enable junk filter logging’.
  5. Haga click en el botón ‘OK’ para cerrar la casilla de verificación ‘Options/Preferences’.

## Alerta y detección de estafas

1. En el cuadro de diálogos Preferences/Options, haga click en ‘Security’ y luego en la pestaña ‘E-mail Scams’.
2. Para que Thunderbird le advierta sobre posibles estafas por correo electrónico, seleccione la casilla de verificación ‘Tell me if the message I’m read is a suspected email scam’. Para desactivar esta característica, desmárquela.
3. Pulse ‘OK’ para cerrar el cuadro de diálogo ‘Options/Preferences’.

## Integración con el antivirus

1. En el cuadro de diálogos Preferences/Options, haga click en ‘Security’ y luego en la pestaña ‘Antivirus’.

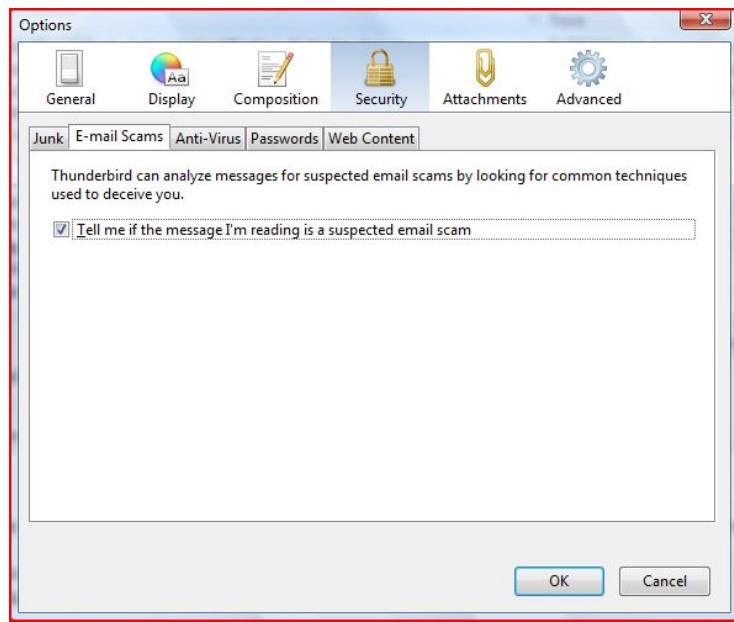


Figure 26.2: Configurando la seguridad

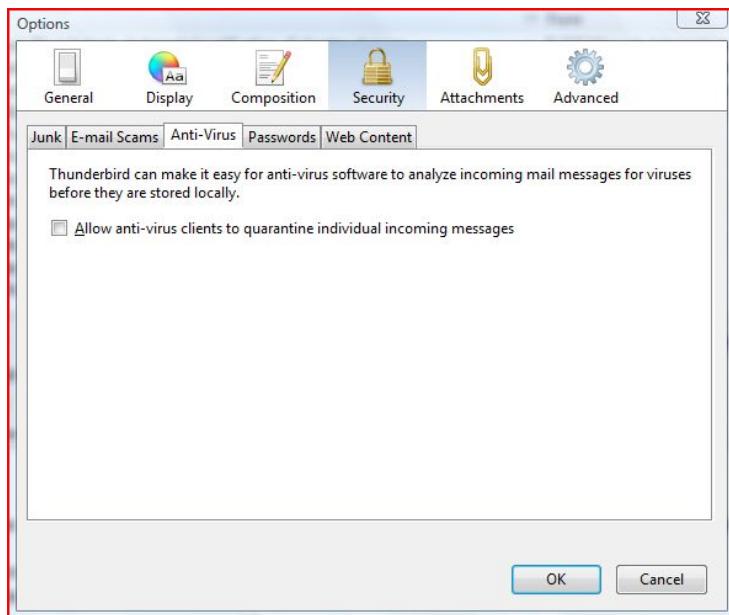


Figure 26.3: Integrando al antivirus

- 
2. Para activar la integración de antivirus, seleccione la casilla de verificación ‘Allow anti-virus clients to quarantine individual incoming messages’. Para desactivar esta característica, desmáquela.
  3. Haga clic en el botón “Aceptar” para cerrar el cuadro de diálogo ‘Options/Preferences’.

## Establezca una contraseña maestra

1. En el cuadro de diálogos Preferences/Options, haga click en ‘Security’ y luego en la pestaña ‘Passwords’.

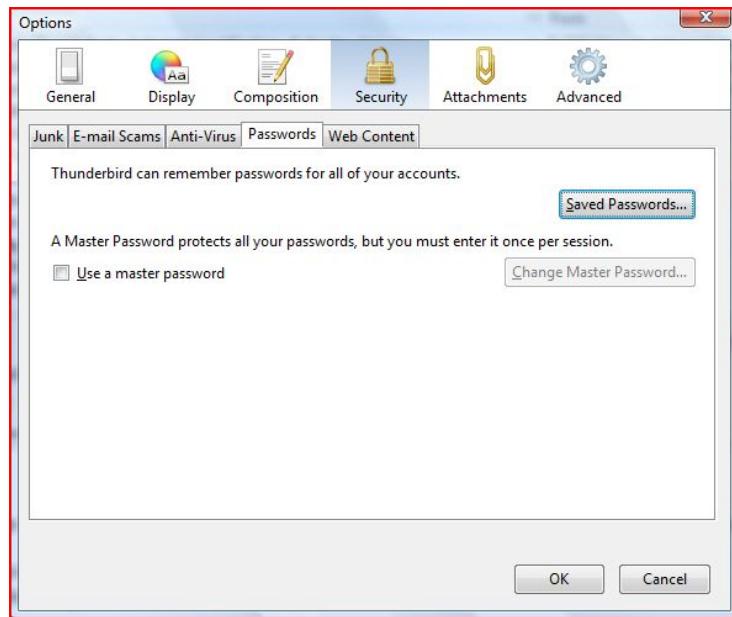


Figure 26.4: Contraseña maestra

2. Seleccione la casilla de verificación ‘Use a master password’.
3. Ingrese su contraseña en los campos ‘Enter new password’ y ‘Re-enter password’.



Figure 26.5: Contraseña

4. Haga click en el botón “OK” para cerrar el cuadro de diálogos Change Master Password.
5. Si desea ver las contraseñas que ha grabado en Thunderbird, haga click en el botón ‘Saved Passwords’. Esto abrirá el cuadro de diálogos ‘Saved Passwords’.
6. Para ver las contraseñas, haga click en el botón ‘Show Passwords’.
7. Haga click en el botón ‘Close’ para cerrar el cuadro de

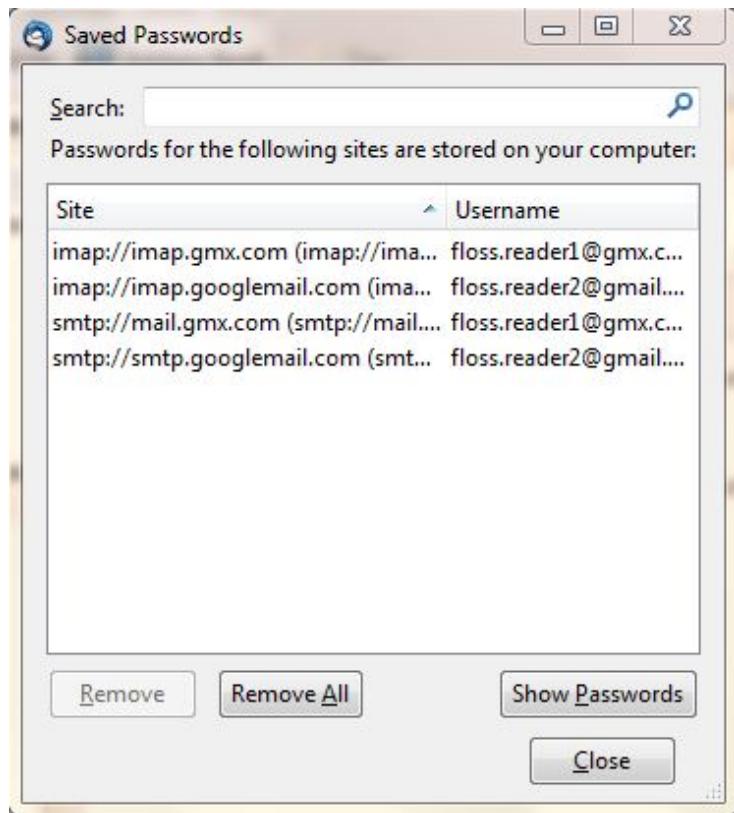


Figure 26.6: Guardando contraseñas

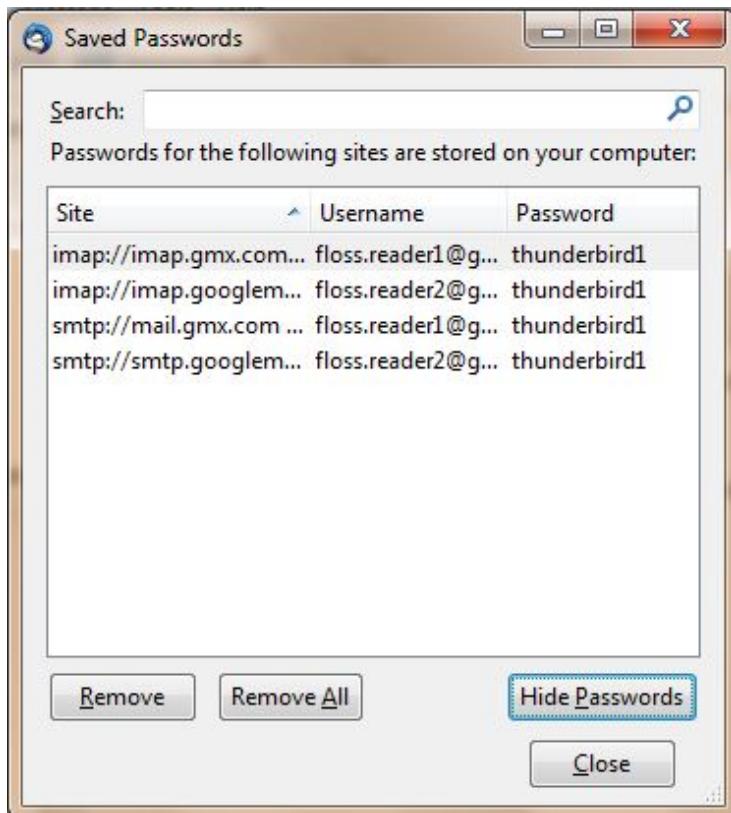


Figure 26.7: Mostrando las contraseñas

- 
- diálogos ‘Saved Passwords’.
8. Haga click en el botón ‘OK’ para cerrar el cuadro de diálogos ‘Options/Preferences’.

## Controles adaptables para correo basura

Necesita primero abrir la ventana de configuración de cuentas (Account Settings). Tenga en cuenta que los ajustes configurados sólo se aplican a la cuenta que haya seleccionado en el panel de carpetas. Debe configurar las carpetas locales por separado.

1. En el panel Carpetas haga clic derecho en un nombre de cuenta y seleccione “Configuración”.
2. En Windows o Mac, vaya al menú ‘Tools’ y seleccione ‘Accounts settings’. En Linux, vaya ‘Edit menu’ y seleccione ‘Account Settings’.
3. Para configurar los controles adaptables de correo basura para una cuenta específica, elija una cuenta y seleccione ‘Junk Settings’.
4. Para activar los controles, seleccione la casilla de verificación “Activar controles adaptables de correo basura para esta cuenta. Para desactivarlos, desmárquela.
5. Si desea que los controles de ignorar el correo de los remitentes en la libreta de direcciones, seleccione las casillas de verificación junto a cualquiera de las libretas de direcciones de la lista.
6. Para usar un filtro de correo como SpamAssassin o SpamPal, active la casilla de verificación denominada ‘Trust junk mail headers sent by:’ y elija un filtro en el menú.

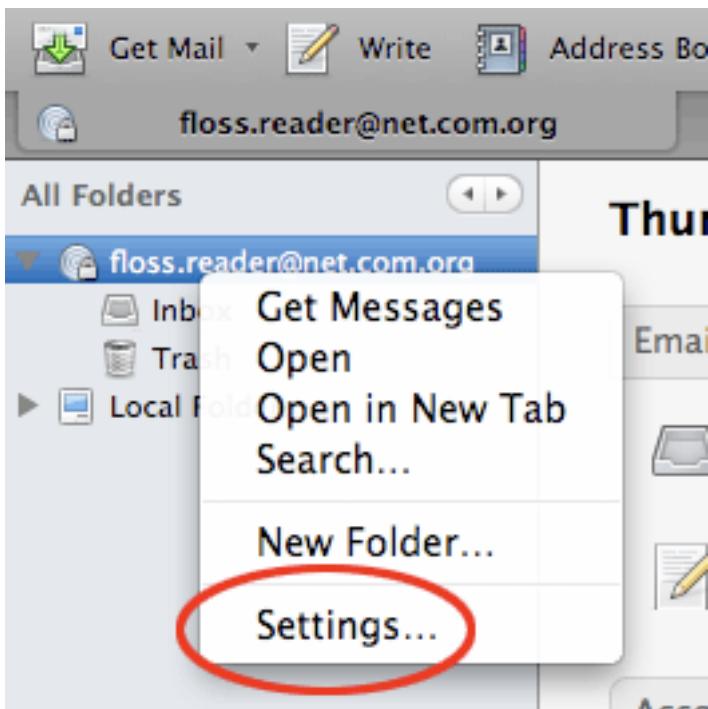


Figure 26.8: Configuración anti spam

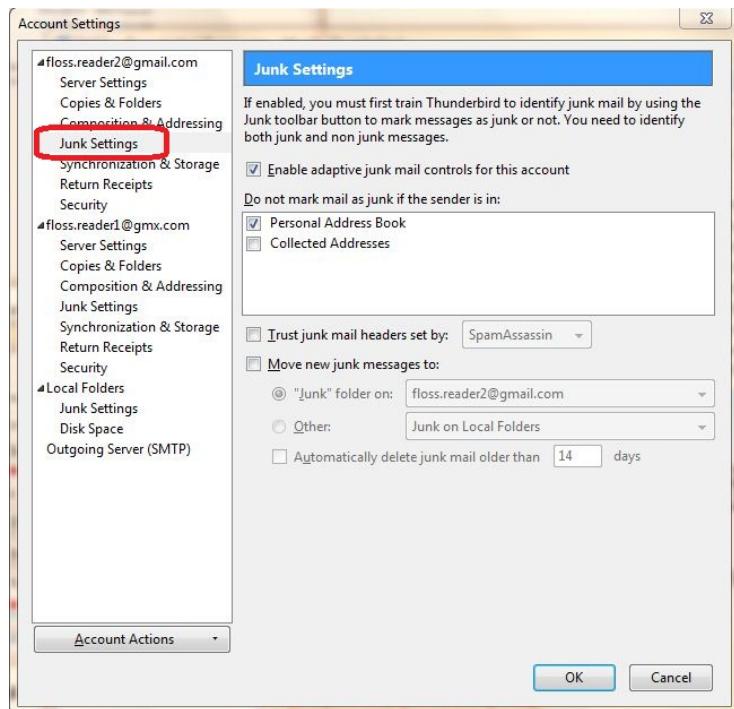


Figure 26.9: Configurando controles adaptables

7. Seleccione la casilla de verificación denominada ‘Move new junk messages to’ si desea mover el correo no deseado a una carpeta especificada. A continuación, seleccione la carpeta de destino para su proveedor de correo electrónico o una carpeta local en el equipo.
8. Seleccione la opción ‘Automatically delete junk mail other 14 days’ en la casilla de verificación para que Thunderbird regularmente elimine los mensajes de correo basura. Para cambiar el período de tiempo para este proceso, introduzca un número diferente (en días) en el cuadro de texto.
9. Haga clic en ‘OK’ para guardar los cambios.

# 27

## Introducción al cifrado de correo electrónico (PGP)

Este capítulo lo introducirá en algunos conceptos básicos acerca de cifrado de correo electrónico. Es importante que lo lea para tener una idea general de cómo funciona, cuáles son sus alcances y cuáles sus limitaciones. **PGP** (Pretty Good Privacy) es el protocolo que se utiliza para cifrar correo electrónico. Este protocolo nos permite firmar digitalmente y cifrar mensajes. Funciona de extremo a extremo: los mensajes se cifran en su propia computadora y sólo pueden ser descifrados por el destinatario del mensaje. No hay posibilidad de que un “man-in-the-middle” lo haga. Esto *excluye* las líneas de ‘asunto’ y las direcciones ‘desde’ y ‘hasta’, que por desgracia no se cifran en este protocolo.

Los siguientes capítulos le proporcionarán una guía práctica para instalar las herramientas necesarias en su sistema operativo y poner en marcha el cifrado. Nos centraremos en el uso de Enigmail que es una extensión para Firefox que lo ayudará a administrar el cifrado PGP para su correo electrónico. El proceso de instalación de Enigmail/PGP es diferente para Mac



Figure 27.1: PGP

---

OSX, Windows y Ubuntu así que por favor consulte los capítulos correspondientes de esta sección para obtener instrucciones.

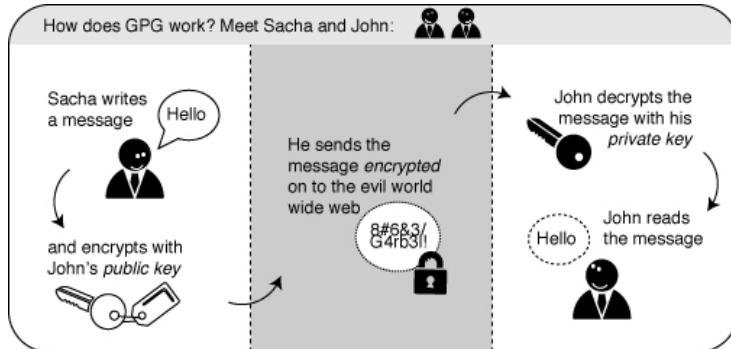


Figure 27.2: GPG Schema

## Uso de un par de claves para cifrar su correo electrónico

Un concepto crucial en el cifrado es el llamado *pares de claves*. Un par de claves son dos archivos separados almacenados en su disco rígido o memoria USB. Siempre que pretenda cifrar mensajes de una cierta cuenta de correo, necesitará disponer de estos archivos de alguna manera. Si los almacena en su computadora, no podrá descifrar mensajes en su trabajo. Una solución posible sería llevarlo en una memoria USB.

Un par de claves consiste de dos claves diferentes: una clave pública y una secreta.

La clave pública: usted puede pasársela a otra persona para que ellos puedan enviarle a usted correos cifrados. Este archivo no se debe mantener en secreto.

La clave secreta: es básicamente su archivo secreto para descifrar mensajes que las personas le envían. No debe darse *nunca* a nadie.

## **Envío de mensajes cifrados a otras personas: usted necesita sus clave públicas**

Si usted tiene compañeros de trabajo y desea enviarles mensajes cifrados necesita la clave pública de cada uno de ellos. Se las podrían enviar por correo electrónico, o podrían dársela en persona, o grabarla en una memoria USB. No importa, siempre que pueda confiar en que esas llaves pertenecen realmente a ellos. Su software pondrá las llaves en su ‘llavero’, por lo que su aplicación de correo sabrá cómo enviar mensajes cifrados.

## **Recepción de mensajes de correo electrónico de otras personas: ellos necesitan su clave pública**

Para que sus compañeros puedan enviarle a *usted* mensajes cifrados, debe distribuir su clave pública a cada uno de ellos.

## **Conclusión: el cifrado de mensajes requiere la distribución de las claves públicas**

Todas las personas de una red de amigos o colegas que esperan enviarse unos a otros mensajes cifrados, necesitan distribuir sus

---

claves públicas unos a otros, mientras mantienen sus claves secretas guardadas en un lugar seguro. El software descripto en este capítulo lo ayudará a administrar sus claves.



# 28

## Instalación de PGP en Windows

Para complicar un poco las cosas, varios programas de software utilizan el protocolo PGP para cifrar correo electrónico. Para trabajar con PGP en Thunderbird necesitamos instalar GPG - una implementación libre de PGP *y* Enigmail - una extensión de Thunderbird que le permite utilizar GPG ... ¿Confundido? No se preocupe por eso, todo lo que tiene que saber es cómo cifrar su correo electrónico con PGP y para eso, necesita instalar a *ambos*, GPG y Enigmail. Ahora explicaremos como hacerlo...

### **Instalación de PGP (GPG) en Microsoft Windows**

Para enviar mensajes cifrados con PGP o para firmarlos, necesitamos el software GNU Privacy Guard (GnuPG). Es necesario instalarlo antes de hacer cualquier tipo de cifrado.

Vaya a la página web del proyecto Gpg4win

En la parte izquierda de la página, encontrará el enlaces a la sección ‘Descargar’. Haga click en él.



Figure 28.1: Página de descarga

Esto le llevará a una página donde se puede descargar Gpg4Win. Haga clic en el botón que le ofrece la última versión estable (no beta).

### Gpg4win 2.1.0

You can download the full version (including the Gpg4win compendium) of Gpg4win 2.1.0 here:



Figure 28.2: Inicio de descarga

Esto descargará un archivo .exe. Dependiendo de su navegador, es posible que tenga que hacer doble clic en el archivo descargado (que se llamará algo así como `gpg4qin-2.1.0.exe`) antes de que algo suceda. Windows le preguntará si está seguro de que desea instalar este programa. Conteste sí.

Luego complete la instalación, aceptando la licencia, seleccionando el idioma apropiado y aceptando las opciones por defecto haciendo clic en ‘Next’, a menos que tenga una razón para no hacerlo.

El programa de instalación le preguntará dónde colocar la aplicación en su computadora. La configuración por defecto debería

---

estar bien, pero tome nota de ella porque es posible que la necesitemos más. Haga clic en “Siguiente” cuando esté de acuerdo.

## Instalación con la extensión Enigmail

Después de haber instalado correctamente el software **PGP** como hemos descrito anteriormente, ahora está listo para instalar el complemento **Enigmail**.

Enigmail es un complemento de Firefox que le permite proteger la privacidad de sus mensajes de correo electrónico. Enigmail es simplemente una interfaz que le permite utilizar el cifrado PGP desde dentro de Thunderbird.

Enigmail se basa en la criptografía de clave pública. En este método, cada individuo debe generar su propio par de claves personales. La primera clave se conoce como la clave privada. Debe estar protegida por una contraseña o frase de acceso, guardada en un lugar secreto y nunca debe compartirse con nadie.

La segunda clave es conocida como la clave pública. Esta clave puede ser compartida con alguno de sus contactos. Una vez que tenga la clave pública del destinatario puede comenzar a enviar mensajes de correo electrónico cifrados a esta persona. Sólo ella será capaz de descifrar y leer sus correos electrónicos, porque ella es la única persona que tiene acceso a la clave privada coincidente.

Del mismo modo, si usted envía una copia de su clave pública propia a sus contactos de correo electrónico y mantiene la correspondiente clave privada en secreto, sólo usted podrá leer los mensajes cifrados de esos contactos.

Enigmail también permite adjuntar firmas digitales a sus mensajes. El destinatario del mensaje que tiene una copia original de su clave pública podrá verificar que el correo electrónico

proviene de usted, y que su contenido no ha sido alterado en el camino. Del mismo modo, si usted tiene la clave pública del destinatario, puede verificar las firmas digitales en sus mensajes.

## Pasos para la instalación

Para empezar a instalar Enigmail, lleve a cabo los siguientes pasos:

1. Abra **Thunderbird**, luego **Select tools > Add-ons** para activar la ventana de complementos, por defecto aparecerá habilitado el panel *Get add-ons*.
2. Ingrese enigmail en la barra de búsqueda, como abajo, y haga click en el ícono de búsqueda.
3. Simplemente haga click en el botón ‘Add to Thunderbird’ para iniciar la instalación.
4. Thunderbird le preguntará si está seguro de que desea instalar este complemento. Confiamos en esta aplicación por lo que debemos hacer click en el botón ‘Install now’.
5. Después de algún tiempo, la instalación se completará y la siguiente ventana debe aparecer. Por favor, haga click en el botón ‘Restart Thunderbird’.

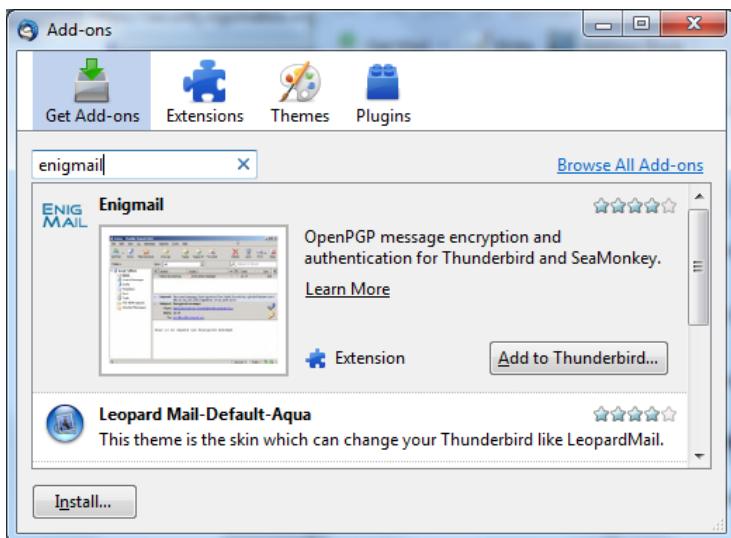


Figure 28.3: Buscando Enigmail

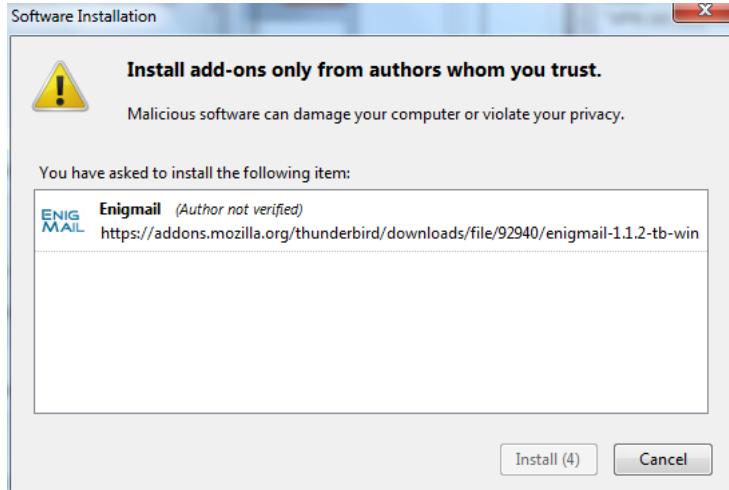


Figure 28.4: Instalando Enigmail

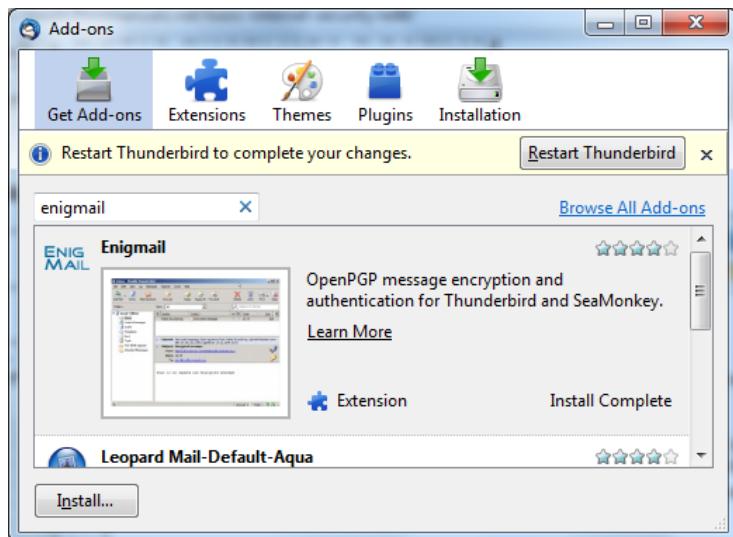


Figure 28.5: Reiniciando



# 29

## Instalación de PGP en OSX

GNU Privacy Guard (GnuPG) es un programa de software que le permite enviar mensajes de correo electrónico cifrados con PGP o firmados. Es necesario instalarlo previamente para poder realizar cualquier tipo de cifrado. Este capítulo cubre los pasos requeridos para instalar GnuPG en Mac OSX.

### Comenzando

En este capítulo supondremos que usted tiene instalado la última versión de:

- OSX (10.6.7)
- Thunderbird (3.1.10)

**Nota acerca de OSX Mail:** Es posible usar PGP con el programa de correo electrónico incorporado de OSX. Sin embargo, no recomendamos esta opción se basa en un hack del programa que no es abierto ni está soportado por su creador, por lo que se rompe con cada actualización del programa de correo. Así que que realmente no tenemos otra opción que recomendarle

cambiar a Mozilla Thunderbird como su programa de correo predeterminado si desea utilizar PGP.

## Descarga e instalación del software

1. Para OSX existe disponible un paquete que instalará todo lo necesario en un solo paso. Para obtenerlo, vaya a gpg-tools y haga click en el gran disco azul con la inscripción “Download GPGTools Installer” debajo. Será redirigido a otra página donde podrá descargar el software.

*(aclaración. estamos usando la última versión de Firefox para este manual, las pantallas pueden lucir algo diferentes si usted usa otro navegador)*

2. Descargue el software seleccionando ‘Save File’ y haciendo click en ‘OK’ en el diálogo.
3. Navegue a la carpeta donde guarda habitualmente sus descargas (generalmente el escritorio o la carpeta de descargas) y haga doble click en el archivo ‘DMG’ para abrir el disco virtual que contiene el instalador.
4. Abra el instalador con un doble click en el ícono.
5. El programa analizará su computadora para determinar si ésta puede ejecutarlo.

(Observe que si su Mac fue construida antes del 2006 no tendrá el procesador de Intel requerido para ejecutar este software y la instalación fallará. Por desgracia, está más allá del alcance de este manual tener también en cuenta a estos equipos de más de cinco años de edad)

Usted será guiado por el programa a través de los pasos siguientes para aceptar el acuerdo de licencia. Presione todo los OK y deténgase al llegar a la pantalla de ‘Tipo de instalación’:



Figure 29.1: Instalando GPG

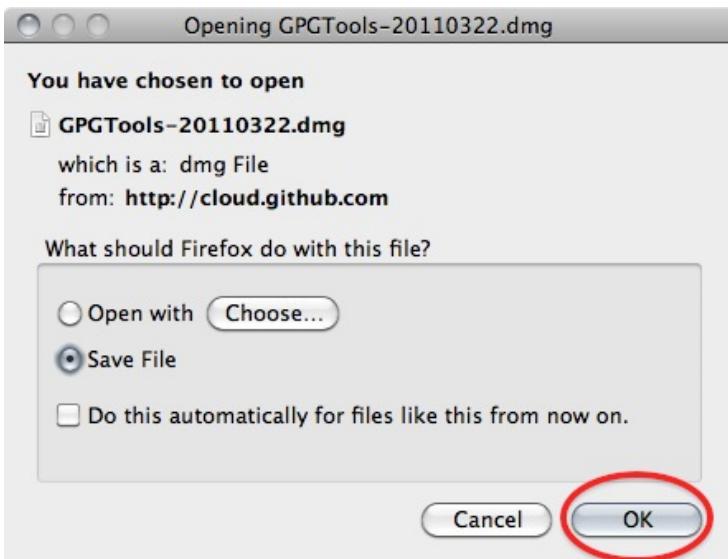


Figure 29.2: Descarga de GPG

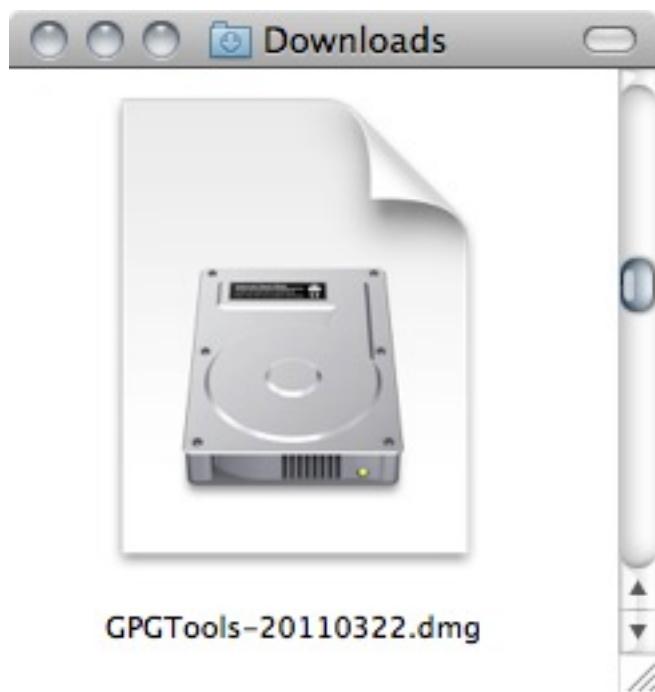


Figure 29.3: Lanzando el instalador



Figure 29.4: Inicio de instalación



Figure 29.5: Observación



Figure 29.6: Tipo de instalación

6. Haga click en ‘Customize’, se abrirá una pantalla donde habrá distintas opciones de programas y software para instalar. Haciendo click en cada uno de ellos tendrá una breve información acerca de qué es, qué hace y por qué puede necesitarlo.

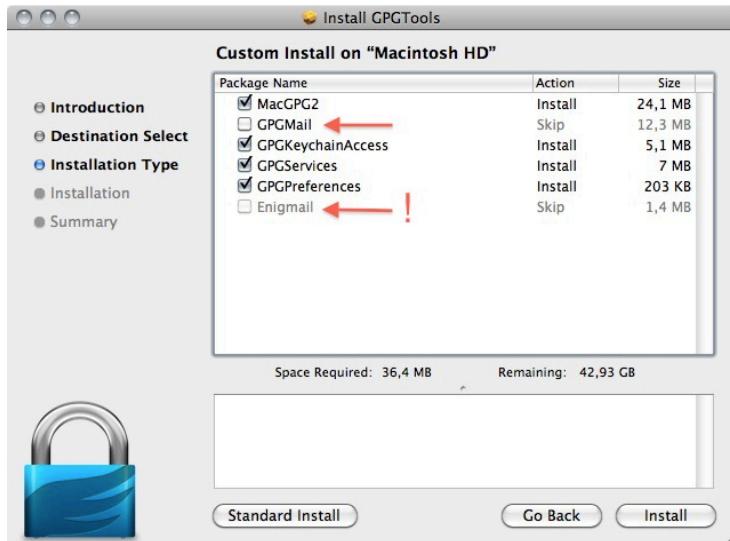


Figure 29.7: Opciones de instalación

Como se dijo en la introducción; advertimos en contrario al uso de Apple Mail en combinación con PGP. Por lo tanto, no va a necesitar ‘GPGMail’, ya que éste habilita PGP en el correo de Apple, y usted puede desactivarlo.

‘Enigmail’ por otra parte es muy importante, ya que es el componente que permitirá a Thunderbird utilizar PGP. En la captura de pantalla aquí es gris vemos como el programa de instalación no pudo identificar mi instalación de Thunderbird. Dicho

---

así parece ser un error. También puede instalar Enigmail desde dentro de Thunderbird como se explica en otro capítulo.

Si la opción no aparece en gris en la instalación, debe funcionar.

Una vez comprobados todos los componentes que desea instalar, haga clic en “Install” para continuar. El instalador le preguntará por su contraseña y después de escribirla la instalación se ejecutará y completará; ¡Hurra!

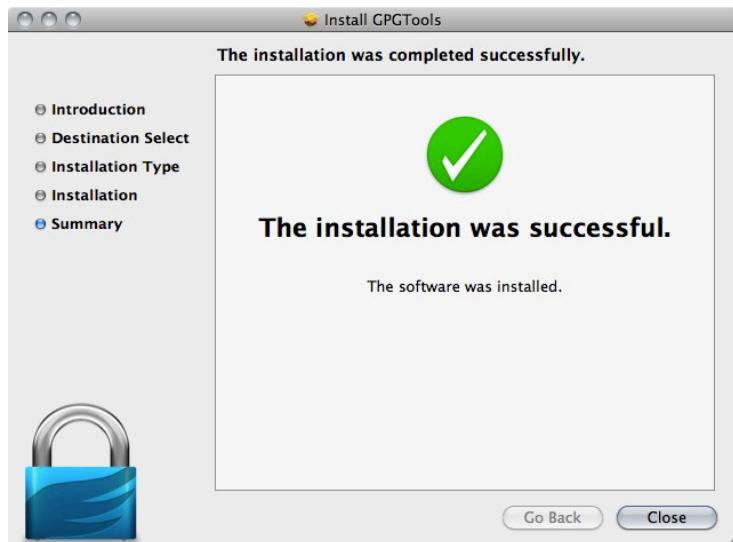


Figure 29.8: Instalando

## Instalación de Enigmail

1. Abra **Thunderbird**, luego **Select Tools > Add-ons** para activar la ventana de los *complementos*; aparecerá

con el panel *Get Add-ons* habilitado por defecto.

2. Despues de abierta la ventana de complementos, busque ‘Enigmail’ e instale la extensión haciendo click en ‘Add to Thunderbird ...’

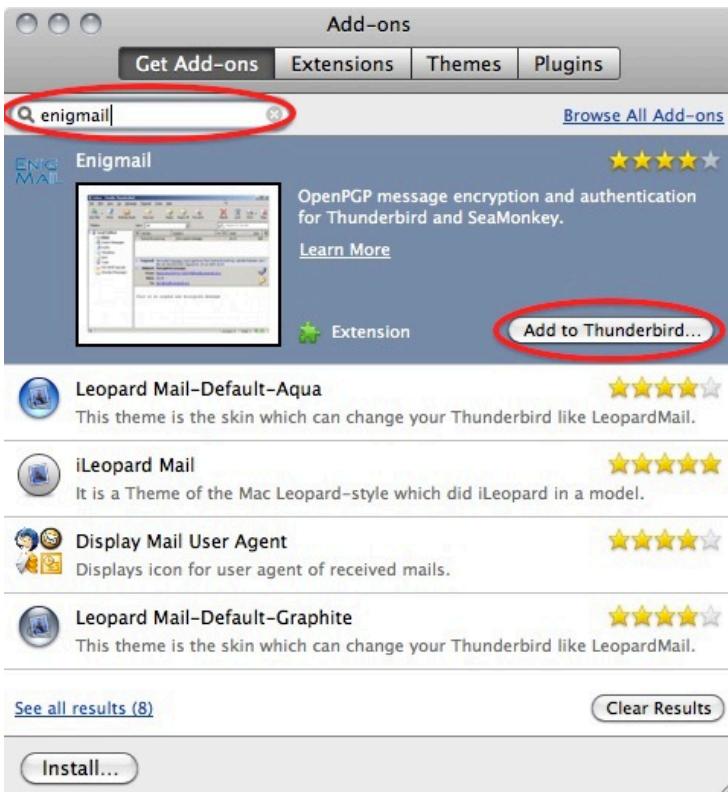


Figure 29.9: Buscando el complemento

3. Haga click en ‘Install Now’ para descargar e instalar la extensión.

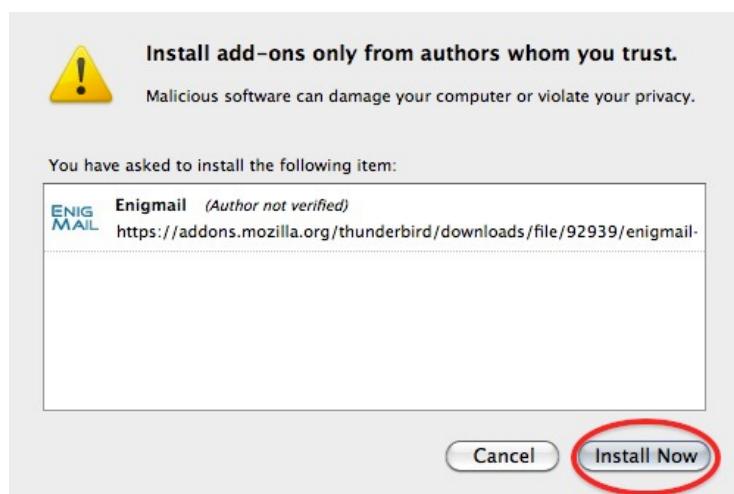


Figure 29.10: Instalando

**¡Tenga en cuenta que deberá reiniciar Thunderbird para usar la funcionalidad de esta extensión!**

Ahora que ha descargado e instalado exitosamente Enigmail y PGP pase al capítulo que trata acerca de cómo configurar el software para su uso.



# 30

## Instalación de PGP en Ubuntu

Usaremos el Ubuntu Software Center para instalar PGP (Enigmail y accesorios). Primero ábralo desde el menú Unity menu tipeando ‘software’ en el área de búsqueda



Figure 30.1: Buscando PGPl

Haga click en el ‘Ubuntu Software Center’.

Tipee ‘Enigmail’ dentro del área de búsqueda, los resultados lo devolverán automáticamente:

Resalte el ítem Enigmail item (debería estarlo por defecto) y

haga click en ‘Install’, se le pedirá autenticar el proceso de instalación.



Figure 30.2: Instalando PGP

Ingrese su contraseña y pulse ‘Authenticate’. El proceso de instalación comenzará.

Cuando el proceso se complete tendrá escasa respuesta desde Ubuntu. La barra de progreso arriba a la izquierda simplemente desaparecerá. El texto ‘In Progress’ a la derecha también desaparecerá. Enigmail debería estar instalado.

# 31

## Instalación de GPG en Android

Con el uso creciente de teléfonos móviles para acceder al correo electrónico, es interesante aprender a usar GPG también en su teléfono. De esta manera, podrá leer sus mensajes en GPG no sólo en su computadora.

Instale las aplicaciones *Android Privacy Guard (APG)* y *K-9 Mail* en su dispositivo Android desde Google Play Store u otra fuente verificada.

1. Genere una nueva clave privada que use DSA-Elgamal con la GPG instalada en su computadora (Sólo se pueden crear claves con una longitud máxima de 1024 bits en Android).
2. Copie la clave privada a su dispositivo Android.
3. Importe la clave privada a APG. Es posible que desee que APG elimine automáticamente la copia en texto plano de la clave privada del sistema de archivos de su dispositivo Android
4. Configure sus cuentas de correo electrónico en *K-9 Mail*.
5. En la configuración de cada cuenta, en *Cryptography*, asegúrese que K-9 Mail sabe cómo usar APG. También puede hacer que K-9 Mail firme automáticamente sus mensajes y/o los descifre si APG puede encontrar una

clave pública para sus destinatarios.

6. Pruébelo.

## APG

Es una pequeña herramienta que hace posible el cifrado GPG en su teléfono. Puede usar APG para administrar sus claves públicas y privadas. Las opciones de la aplicación son bastante sencillas si tiene algún conocimiento en GPG.

La administración de claves no está bien muy implementada aún. La mejor manera es copiar manualmente sus claves públicas en una tarjeta SD en la carpeta de APG. Entonces será muy sencillo importar sus claves. Después que las haya importado, cifrado con GPG, firmado y descifrado estarán disponibles para otras aplicaciones siempre y cuando estén integradas con el cifrado/GPG.

## Cómo habilitar GPG en correos electrónicos en Android: K-9 Mail

La aplicación de correo no soporta GPG por defecto. Afortunadamente existe una alternativa excelente: K-9 Mail. Esta aplicación está basada en la aplicación original de Android pero con algunas mejoras. La aplicación puede utilizar APG, ya que es proveedor de GPG. La configuración de K-9 Mail es sencilla y similar a la configuración del correo electrónico en la aplicación de Android por defecto. En el menú de configuración hay una opción para habilitar “Cryptography” para la firma del correo GPG.

---

Si desea tener acceso a su correo electrónico en su teléfono GPG esta aplicación es una necesidad.

Por favor, note que debido a algunos errores pequeños en K-9 Mail y/o APG, es muy recomendable deshabilitar el correo HTML y utilizar sólo texto sin formato. Los mensajes del tipo HTML no están bien cifrados y a menudo son ilegibles.



# 32

## Creación de sus claves PGP

Enigmail presenta un agradable asistente que le ayudará a crear su par de claves pública/privada (vea el capítulo Introducción a PGP para una explicación). Puede iniciar el asistente en cualquier momento dentro de Thunderbird seleccionando **OpenPGP > Setup Wizard** desde el menú superior.

1. Así luce el asistente. Por favor, lea el texto en todas las ventanas con cuidado. Proporciona información útil y lo ayudará a configurar PGP de acuerdo con sus preferencias personales. En la primera pantalla, haga click en **Next** para iniciar la configuración.
2. El asistente le preguntará si desea firmar todos los mensajes de correo salientes. La firma de todos los mensajes es una buena opción. Si usted no la elige, todavía puede decidir hacerlo de forma manual para firmar un mensaje cuando lo está redactando. Haga clic en el botón ‘**Next**’ una vez que haya tomado una decisión.
3. En la siguiente pantalla, el asistente le preguntará si desea cifrar *todos* los mensajes de correo salientes. A diferencia de la firma de correo electrónico, el cifrado requiere

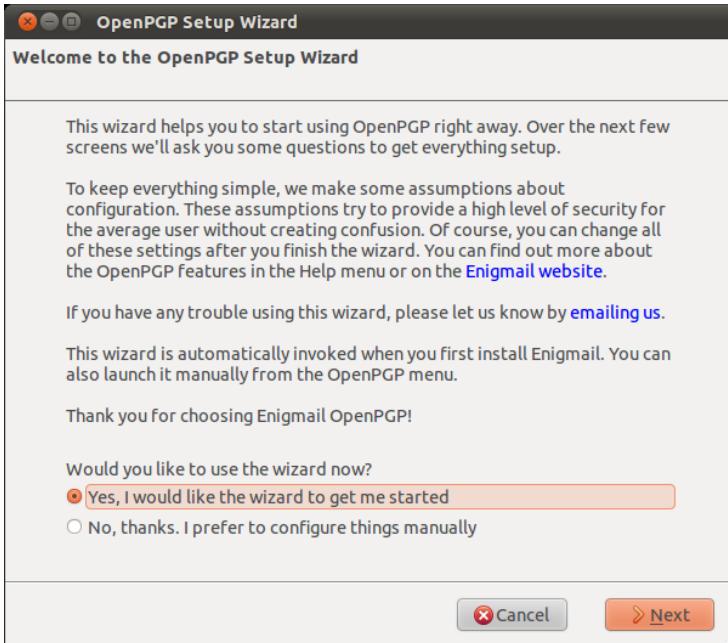


Figure 32.1: Inicio

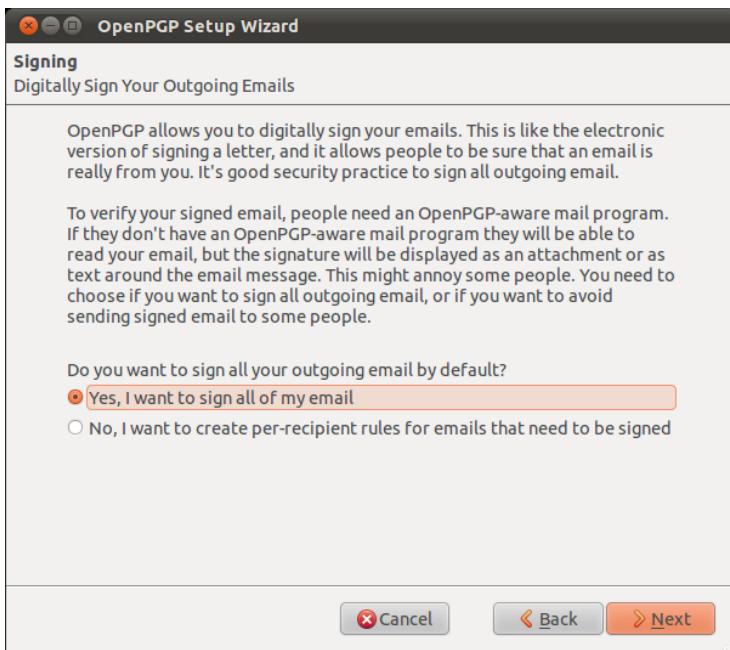


Figure 32.2: Opciones de firma

que el destinatario disponga de software de PGP instalado. Probablemente debería responder ‘no’ a esta pregunta, por lo que se va a enviar normal (sin cifrar) de correo por defecto. Una vez que haya tomado su decisión, haga clic en el botón ‘Next’.



Figure 32.3: Opciones de cifrado

4. En la siguiente pantalla el asistente le preguntará si quiere cambiar algo en su configuración del formato del correo para trabajar mejor con PGP. Es una buena opción responder ‘Sí’ aquí. Esto significa que, por defecto, el correo estará integrado en texto sin formato en lugar de HTML. Haga clic en el botón ‘Next’ después de que usted haya

tomado su decisión.

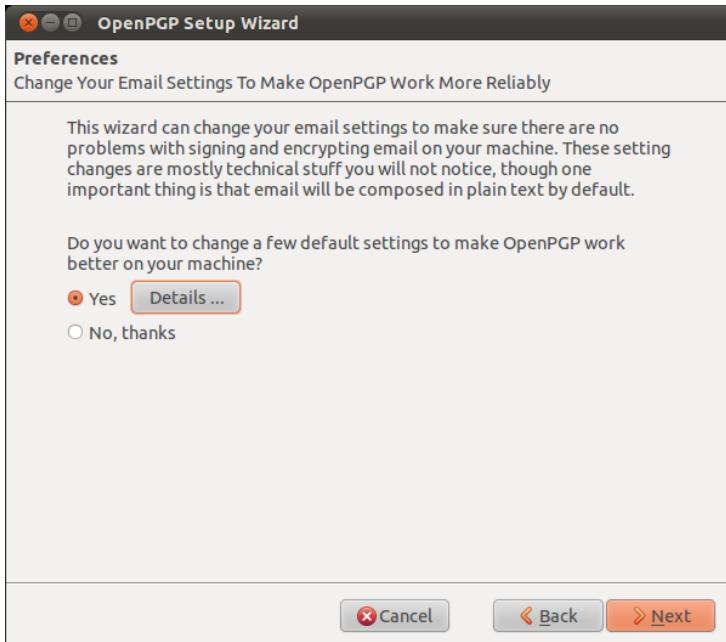


Figure 32.4: Formato de correo

5. En la siguiente pantalla, seleccione una de las cuentas de correo. En el cuadro de texto 'Contraseña' debe introducir una. Se trata de un nuevo archivo *contraseña* que se utiliza para proteger su clave privada. Es **muy importante** recordar esta contraseña, ya que no puede leer sus mensajes de correo electrónico cifrados propios en caso de olvido. Debe ser una contraseña **fuerte**, lo ideal es 20 caracteres o más. Por favor, vea el capítulo sobre las contraseñas para obtener ayuda sobre la creación de contraseñas únicas, largas y fácil de recordar. Una vez

seleccionada una su cuenta creada una contraseña, haga click en el botón “Siguiente”.

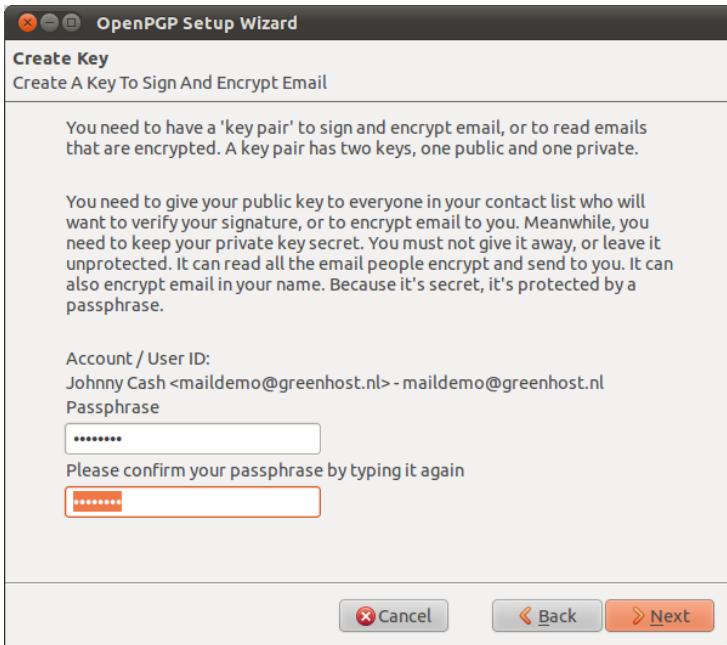


Figure 32.5: Selección de cuenta

6. En la siguiente pantalla del asistente resume las acciones que tomará para habilitar el cifrado PGP para su cuenta. Si está satisfecho, haga clic en el botón “Siguiente”.
7. Sus claves serán creados por el asistente, que tomará algún tiempo. Cuando se haya completado, haga clic en el botón “Siguiente”.
8. Ahora tiene su propio par de claves PGP. El asistente le preguntará si también desea crear un “certificado de re-

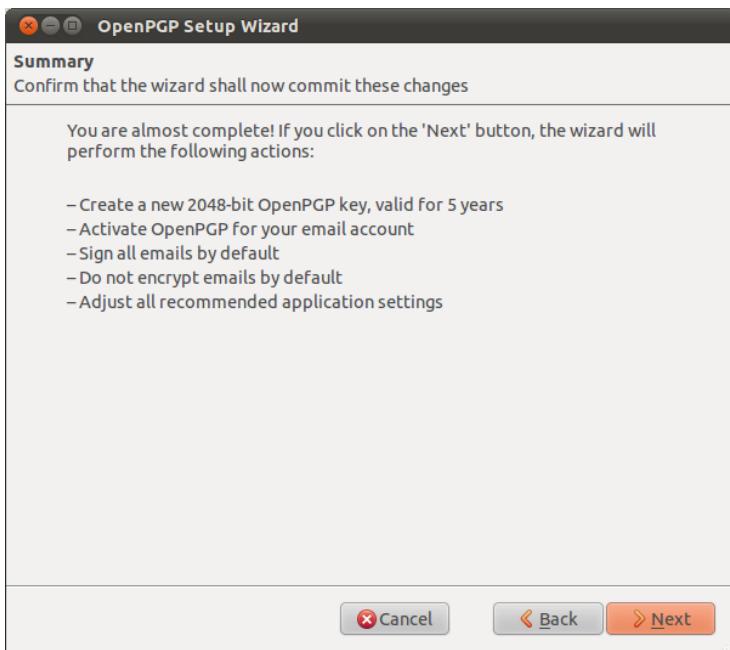


Figure 32.6: Resumen de acciones a tomar

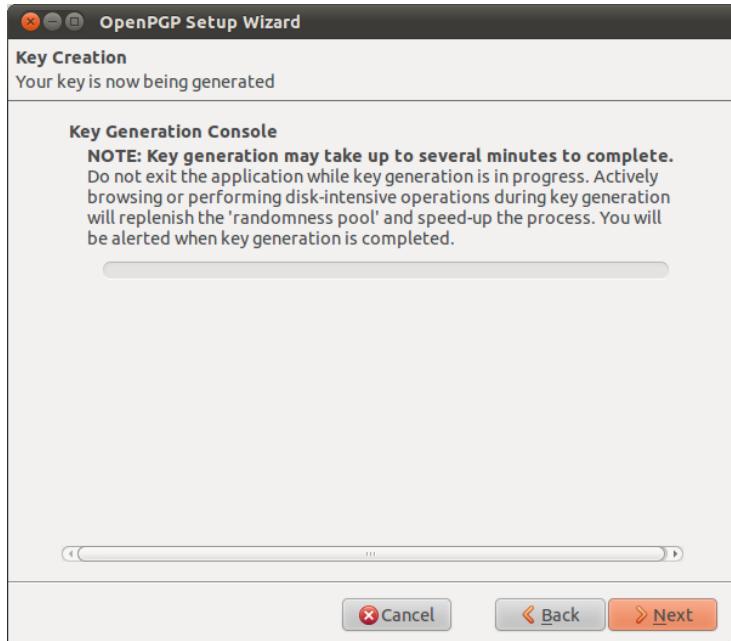


Figure 32.7: Creación de claves

---

vocación. Este es un archivo que se puede utilizar para informar a todo el mundo si la clave privada está en peligro, por ejemplo, si su portátil es robado. Piense en ello como un “kill switch” para su identidad PGP. Usted también puede desear revocar la clave, simplemente porque usted ha generado una nueva, y el viejo es obsoleto.

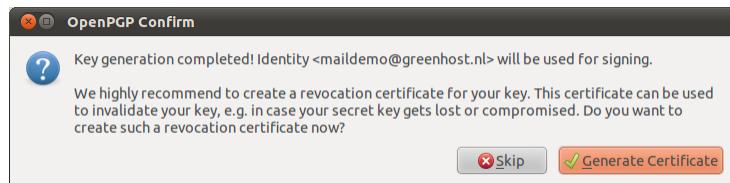


Figure 32.8: Certificado de revocación

9. Si ha decidido generar un certificado de revocación, el asistente le pedirá la ubicación del archivo debe ser guardado. El diálogo tendrá un aspecto diferente dependiendo del sistema operativo que utilice. Es una buena idea cambiar el nombre del archivo a algo sensato como *my\_revocation\_certificate*. Haga clic en “Guardar” cuando usted haya decidido sobre un lugar.

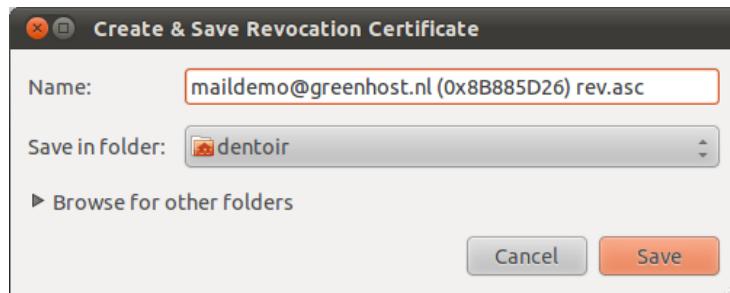


Figure 32.9: Guardando el certificado

10. Si ha decidido generar un certificado de revocación, el asistente le informa de que se ha almacenado correctamente. Si lo desea, imprimirlo o grabarlo en un CD y guárdelo en un lugar seguro.

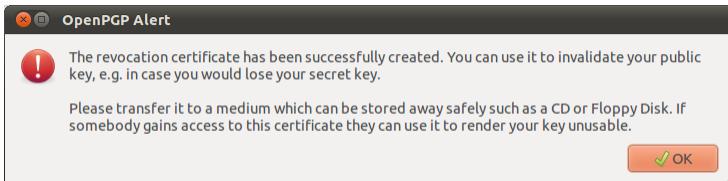


Figure 32.10: Confirmación

11. El asistente le informará de que ha completado.

Felicitaciones, ahora tiene un cliente de correo electrónico totalmente configurado con PGP. En el próximo capítulo vamos a explicar cómo manejar sus llaves, mensajes de muestra y hacer la encriptación. Thunderbird puede ayudarle a hacer un montón de estas cosas automáticamente. Uso cotidiano de GPG  
=====

En los capítulos previos hemos explicado como configurar un ambiente seguro para el correo electrónico usando Thunderbird, GPG y Enigmail. Asumiremos que ya tiene instalado el software mencionado y que ha seguido exitosamente y paso a paso las instrucciones del asistente para generar un par de claves de cifrado como se describió anteriormente. Este capítulo explicará como usar Thunderbird en forma segura cotidianamente para proteger sus comunicaciones por correo electrónico. En particular, nos enfocaremos en:

1. Cifrado de archivos adjuntos
2. Ingreso de una frase de paso
3. Recepción de mensajes cifrados
4. Envío y recepción de claves públicas

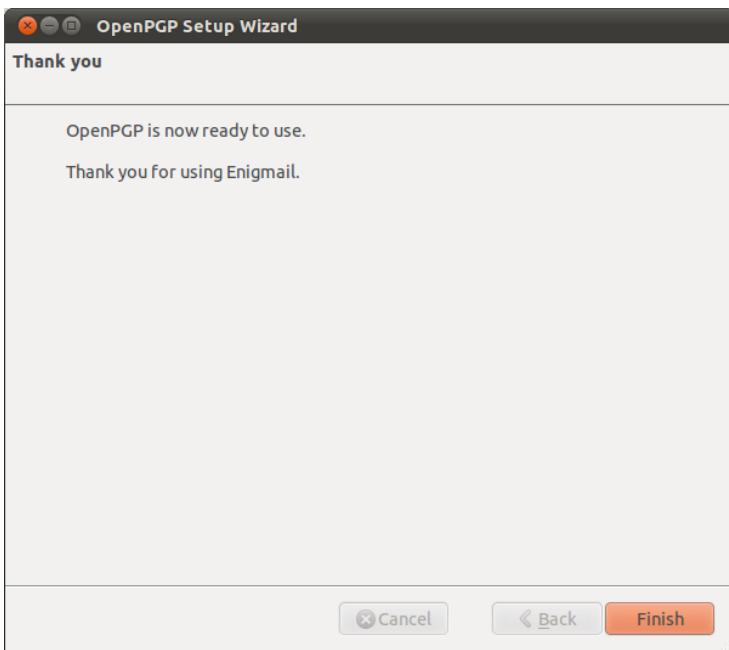


Figure 32.11: Finalizando

5. Recepción de claves públicas y agregado de las mismas a su anillo de claves
6. Uso de servidores de claves públicas
7. Firma de un mensaje en particular
8. Envío de mensajes cifrados a una destinatario en particular
9. Cifrado automático para destinatarios específicos
10. Verificación de mensajes entrantes
11. Revocación de su par de claves GPG
12. Qué hacer si pierde su clave secreta, u olvida la frase de paso
13. Qué hacer si robaron su clave secreta, o si la misma está comprometida
14. Copias de resguardo de sus claves

Primero vamos a explicar dos ventanas de diálogo que inevitablemente aparecen después de empezar a usar Thunderbird para cifrar sus correos electrónicos.

## Cifrado de archivos adjuntos

La ventana de diálogo siguiente aparece cada vez que se envía un correo electrónico con archivos adjuntos cifrados por primera vez. Thunderbird hace una pregunta técnica sobre cómo cifrar los archivos adjuntos en el correo. La opción predeterminada (la segunda) es la mejor opción, ya que combina la seguridad con la máxima compatibilidad. También debe seleccionar la opción ‘Use the selected method for all future attachments’. A continuación, haga click en ‘Aceptar’ y su correo será enviado de inmediato.

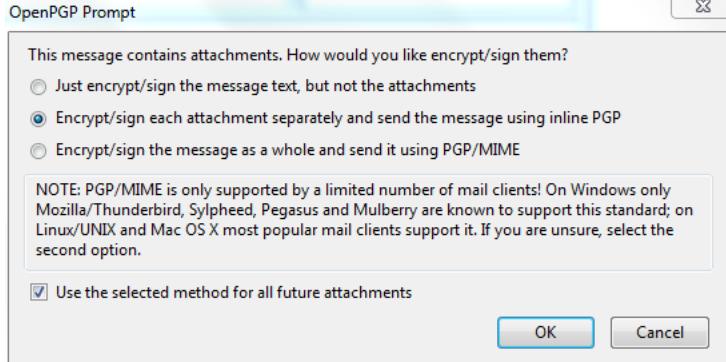


Figure 32.12: Forma de cifrado

## Ingreso de una frase de paso

Por razones de seguridad, la frase de paso para su clave secreta se almacena temporalmente en la memoria. De vez en cuando la ventana de diálogo siguiente aparecerá. Thunderbird le pide la frase de paso para su clave secreta. Esto debe ser diferente de su contraseña de correo electrónico normal. Es la frase de paso que ha introducido al crear el par de claves en el capítulo anterior. Introduzca la frase de paso en el cuadro de texto y haga click en 'OK'

## Recepción de mensajes cifrados

El descifrado de mensajes de correo electrónico es manejado automáticamente por Enigmail, la única acción que tendrá que hacer eventualmente es introducir la frase de paso para su clave secreta. Sin embargo, para mantener cualquier tipo de correspondencia cifrada con alguien, primero tienen que intercambiar

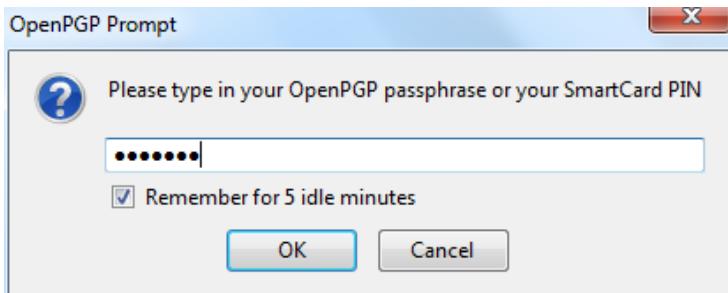


Figure 32.13: Frase de paso

sus claves públicas.

## Envío y recepción de claves públicas

Existen varias formas de distribuir su clave pública a los amigos o compañeros de trabajo. Con mucho, la forma más simple consiste en adjuntar su clave a un correo electrónico. Para que su lista de amigos pueda confiar en que el mensaje procede realmente de usted, debe informarles en persona (si es posible) y también obligarles a que respondan a su correo. Esto debería al menos evitar falsificaciones fáciles. Usted tiene que decidir por sí mismo cuál es el nivel de la validación necesario. Esto también es válido cuando se reciben mensajes de correo electrónico de terceros que contienen las claves públicas. Póngase en contacto con su interlocutor a través de algún medio de comunicación alternativo. Puede utilizar un teléfono, mensajes de texto, voz sobre protocolo de Internet (VoIP) o cualquier otro método, pero debe estar absolutamente seguro de que usted está realmente hablando con la persona correcta. Como resultado de ello, las conversaciones telefónicas y reuniones cara a cara fun-

---

cionan mejor, si ellas son convenientes y si se pueden organizar de manera segura.

El envío de la clave pública es simple



1. En Thunderbird, pulse el ícono
2. Envíe un mensaje a su amigo o colega y dígale que le ha enviado su clave PGP pública. Si sus amigos no saben qué significa esto, debe explicárselo y referirles alguna documentación.
3. Antes de enviar el correo, haga clic en la opción `OpenPGP> Adjuntar mi clave pública` en la barra de menús de la ventana de redacción de correo. Junto a esta opción aparecerá un signo marcado. Vea el siguiente ejemplo.



4. Envíe su correo haciendo click en el botón

## Recepción de claves públicas y agregado de las mismas a su anillo de claves

Supongamos que recibe una clave pública de un amigo por correo. La clave se mostrará en Thunderbird como un *archivo adjunto*. Desplácese por el mensaje y por debajo verá las pestañas con uno o dos nombres de archivo. La extensión de este archivo de clave pública será .asc, a diferencia de la extensión de un archivo adjunto de firma GPG, que termina en .asc.sig

Observe el ejemplo de correo electrónico en la imagen siguiente, que es un mensaje GPG recibido firmado que contiene una clave pública adjunta. Verá una barra amarilla con un mensaje de

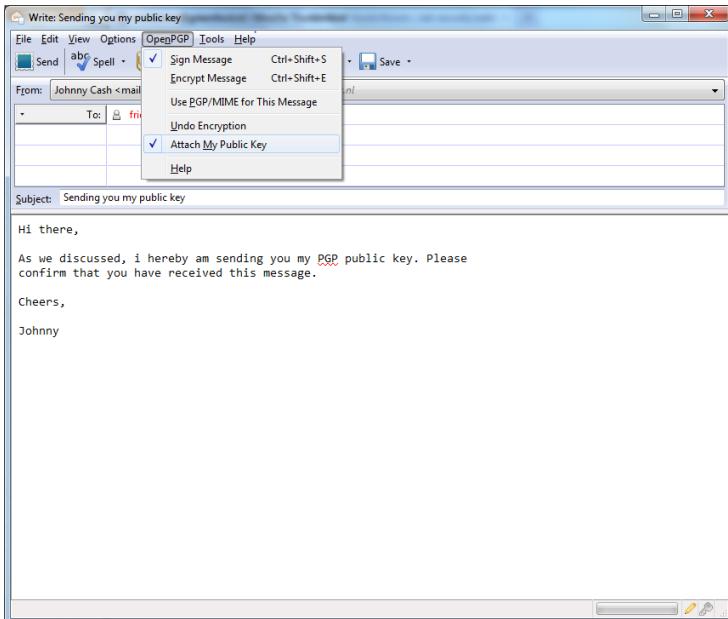


Figure 32.14: Opción de envío

---

advertencia: ‘OpenPGP: Unverified signature, click on ‘Details’ button for more information’. Thunderbird nos advierte de que el remitente no se conoce todavía, lo que es correcto. Esto va a cambiar una vez que aceptemos la clave pública.

¿Qué están haciendo todos esos caracteres extraños en el mensaje de correo? Debido a que Thunderbird aún no reconoce la firma como válida, se imprime la firma cruda entera, al igual que lo que ha recibido. Así es como aparecerán los mensajes GPG firmados digitalmente a todos aquellos destinatarios que no tengan su clave pública.

Lo más importante en este caso es encontrar la clave pública GPG adjunta. Hemos mencionado que es un archivo que termina en .asc. En este ejemplo, es el primer archivo adjunto a la izquierda, en el círculo rojo. Si hace doble clic sobre este archivo adjunto, Thunderbird reconocerá la clave.

Después de hacer click en el archivo adjunto, la siguiente ventana aparecerá.

Thunderbird ha reconocido el archivo de clave pública GPG. Seleccione ‘Import’ para añadir esta clave a su anillo. La siguiente ventana aparecerá. Thunderbird le indica que la operación ha sido exitosa. Pulse ‘OK’.

De vuelta en la pantalla principal de Thunderbird, actualizamos la vista de este ejemplo de mensaje en concreto, haciendo clic en algún otro mensaje. Ahora, el cuerpo del mensaje se ve diferente (véase más adelante). Esta vez Thunderbird *podrá* reconocer la firma, ya que hemos añadido la clave pública del remitente.

Aún falta algo. Aunque Thunderbird reconoce ahora la firma, debemos verificar explícitamente que la clave pública realmente pertenece al remitente en la vida real. Nos damos cuenta de esto cuando echamos un vistazo más de cerca a la barra verde (ver más abajo). Si bien la firma es buena, todavía no es confiable.

Si decide confiar en esta clave pública particular y las firmas

## Creación de sus claves PGP

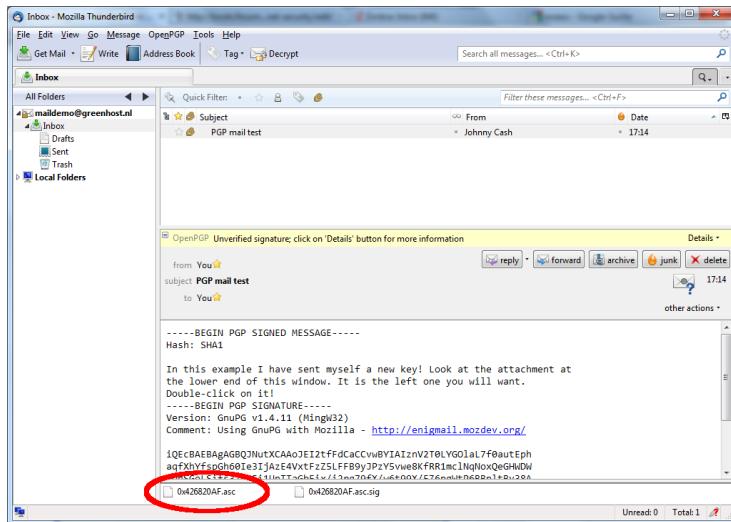


Figure 32.15: Clave GPG adjunta

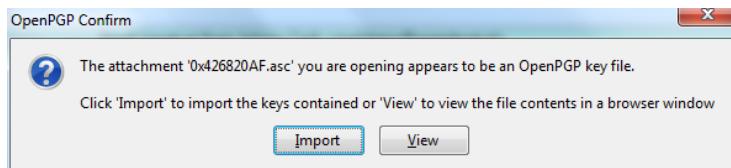


Figure 32.16: Ventana de confirmación

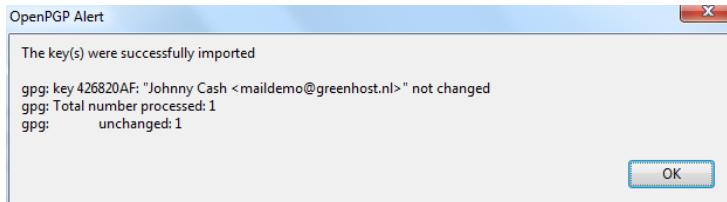


Figure 32.17: Importación de clave pública

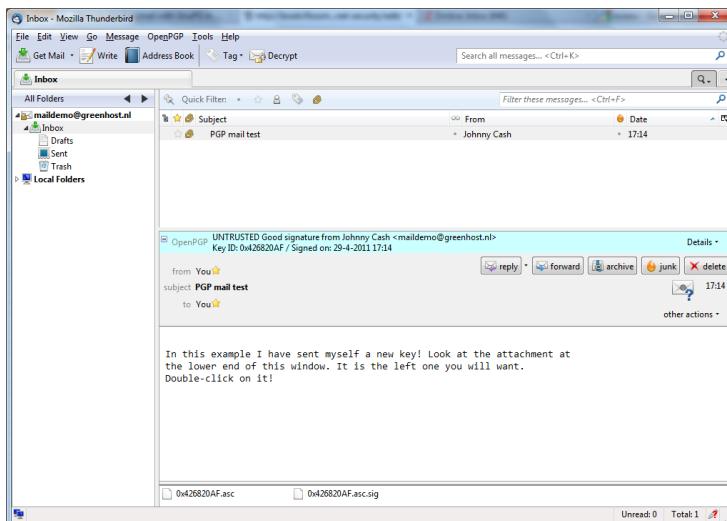


Figure 32.18: Reconocimiento de la firma



Figure 32.19: Verificando la confianza

hechas por ella, haga click en ‘Details’. Un pequeño menú aparecerá (ver más abajo). Desde este menú se debe hacer click en la opción ‘Sign Sender’s Key ...’.

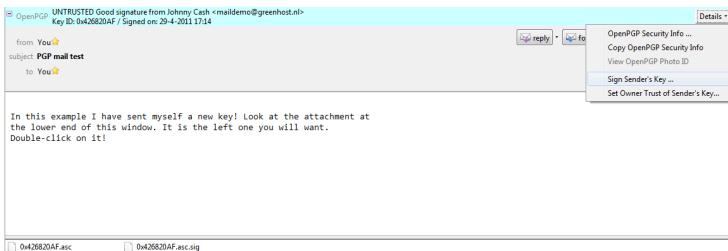


Figure 32.20: Detalles

Después de elegir ‘Sign Sender’s Key ...’ aparecerá otra ventana de selección (ver más abajo). Nos pedirá que indiquemos qué tan cuidadosamente hemos seleccionado esta clave para su validez. La explicación de los niveles de confianza y redes de confianza en GPG queda fuera del alcance de este documento. No utilizaremos esta información, por lo tanto, nos limitaremos a seleccionar la opción ‘I will not answer’ (“No voy a responder”). También seleccione la opción ‘Local signature (cannot be exported)’. Haga click en el botón “Aceptar” para terminar de firmar esta clave. Esto completa la aceptación de la clave pública. Ahora puede enviar correo cifrado a este individuo.

## Uso de servidores de claves públicas

Otro método para distribuir claves públicas es colocarlas en un servidor. Esto permite que cualquier persona pueda comprobar si su dirección de correo electrónico soporta GPG, y luego descargar su clave pública.

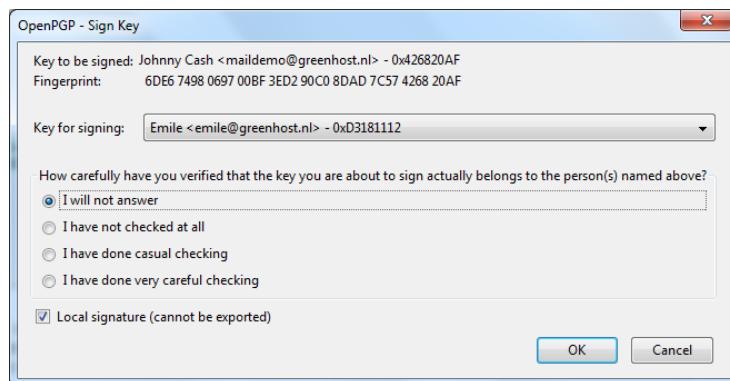


Figure 32.21: Aceptación de la clave

Para guardar su propia clave en un servidor, haga lo siguiente:  
i 1. Diríjase hacia el administrador de claves utilizando el menú de Thunderbird y haga click en OpenPGP > Key Management

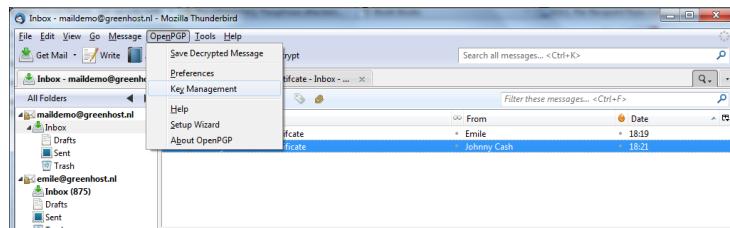


Figure 32.22: Administración de claves

2. Aparecerá la siguiente ventana:
3. Seleccione ahora la opción 'Display All Keys by Default' para acceder a la lista de todas sus claves. Busque su dirección de correo electrónico en la lista y haga click derecho. Aparecerá una ventana de selección con algunas opciones.

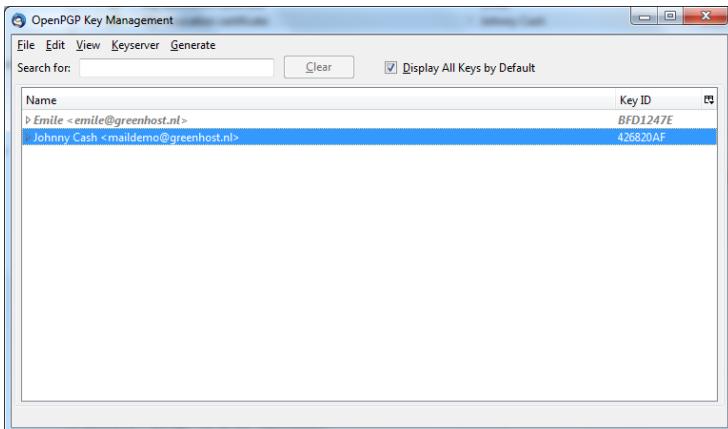


Figure 32.23: Ventana de administración

Elija ‘Upload Public Keys to Keyserver’.

4. Ahora verá una pequeña ventana de diálogo. El servidor por defecto para distribuir sus claves es correcto. Presione ‘OK’ y distribuya su clave pública por el mundo.

Para saber si alguna dirección de correo electrónico posee una clave pública disponible, siga los siguientes pasos:

1. Diríjase al administrador de claves mediante el menú de Thunderbird y seleccione **OpenPGP > Key Management**
2. En la barra de menú de la ventana del administrador de claves, seleccione **Keyserver > Search for Keys**
3. En este ejemplo buscaremos 1 clave del creador del software PGP, Philip Zimmermann. Después de ingresar la dirección de correo electrónico, pulse ‘OK’.
4. La ventana próxima mostrará el resultado de nuestra búsqueda. Nosotros hemos encontrado la clave pública.

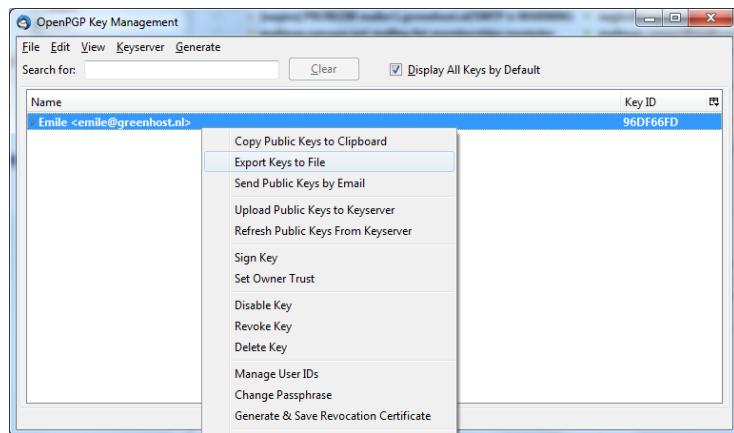


Figure 32.24: Selección de opciones

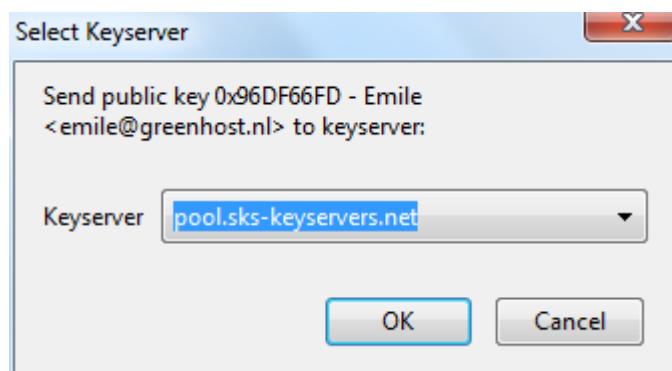


Figure 32.25: Distribución de claves

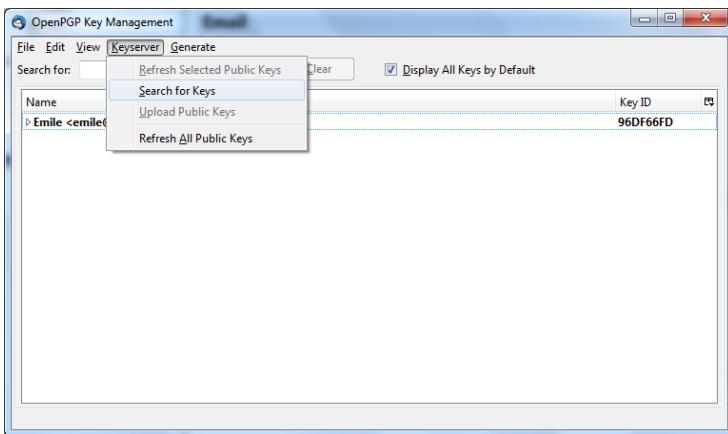


Figure 32.26: Búsqueda de claves

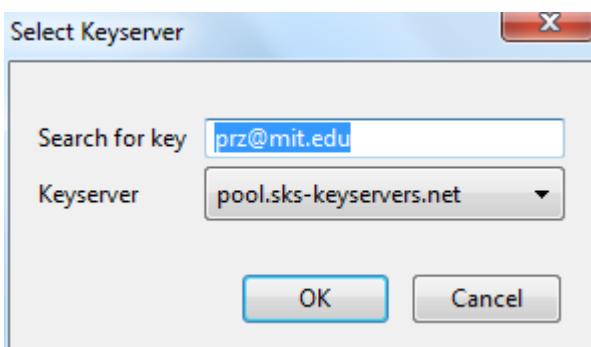


Figure 32.27: Buscando...

---

Se ha seleccionado automáticamente. Solo presione ‘OK’ para importar la clave.

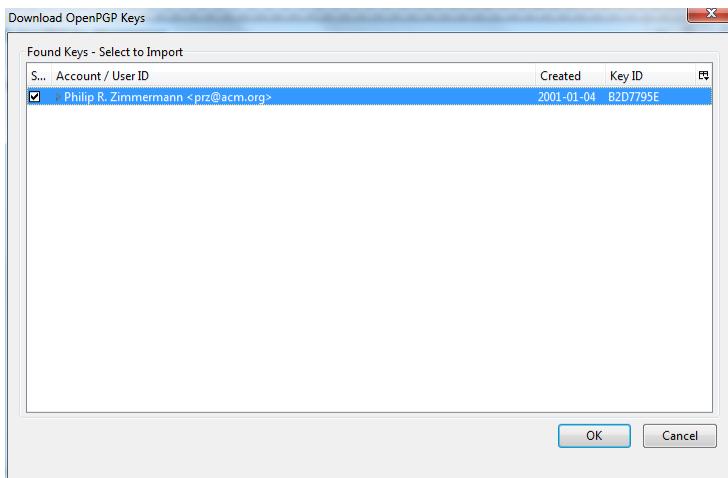


Figure 32.28: Claves halladas

5. Importar la clave tomará algo de tiempo. Al completarse, se debería mostrar una ventana como la siguiente:
6. El paso final es firmar localmente la clave, para indicar que confiamos en ella. Cuando esté de vuelta en el gestor de claves, asegúrese de que ha seleccionado la opción ‘Display All Keys by Default’. Ahora debería ver la clave recién importada en la lista. Haga click en la dirección y seleccione ‘Key Sign’.
7. Seleccione ‘I will not answer’ y ‘Local signature (cannot be exported)’, luego pulse ‘OK’. Ya puede enviarle correo cifrado a Philip Zimmermann.

## Creación de sus claves PGP

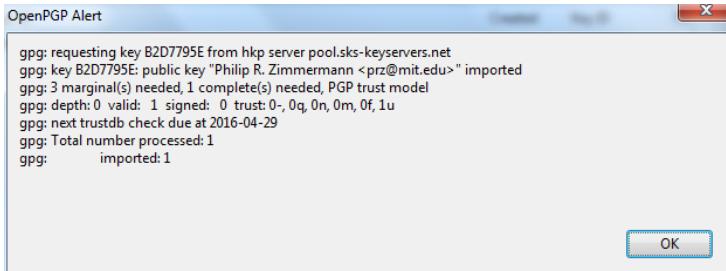


Figure 32.29: Clave importada

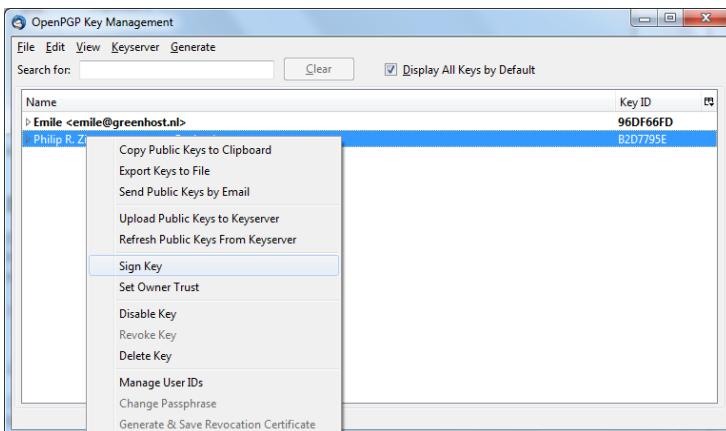


Figure 32.30: Firmando la clave localmente

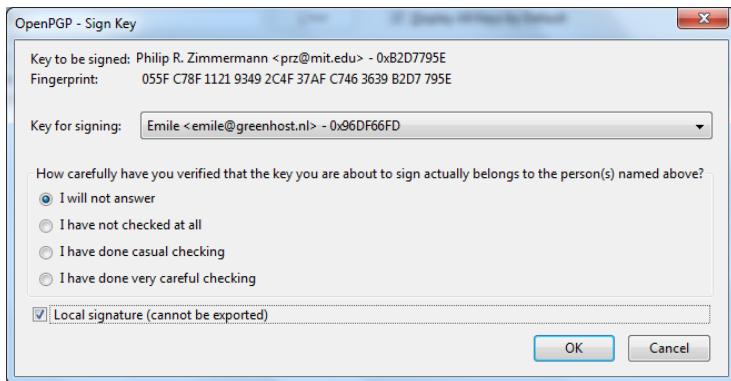


Figure 32.31: Aceptando

## Firma de un mensaje en particular

Firmar digitalmente sus mensajes es la manera de probar al destinatario que usted los ha enviado. Quienes reciban su clave pública serán capaces de *verificar* que su mensaje es auténtico. Sin embargo, tome nota que firmar un mensaje hará que sea muy difícil (si no imposible) negar que usted ha sido el autor del mensaje.

1. Ofrezca a sus amigos su clave pública, usando los métodos descriptos anteriormente en este capítulo.
2. En Thunderbird, pulse en el ícono *Write*.
3. Antes de enviar el mensaje, habilite la opción **OpenPGP > Sign Message** desde la barra de menú de la ventana de redacción del mensaje, si aún no está habilitado. Luego, pulse sobre la opción y aparecerá una firma marcada. Al hacer otro click, debería deshabilitarse el cifrado. Vea el ejemplo más abajo:

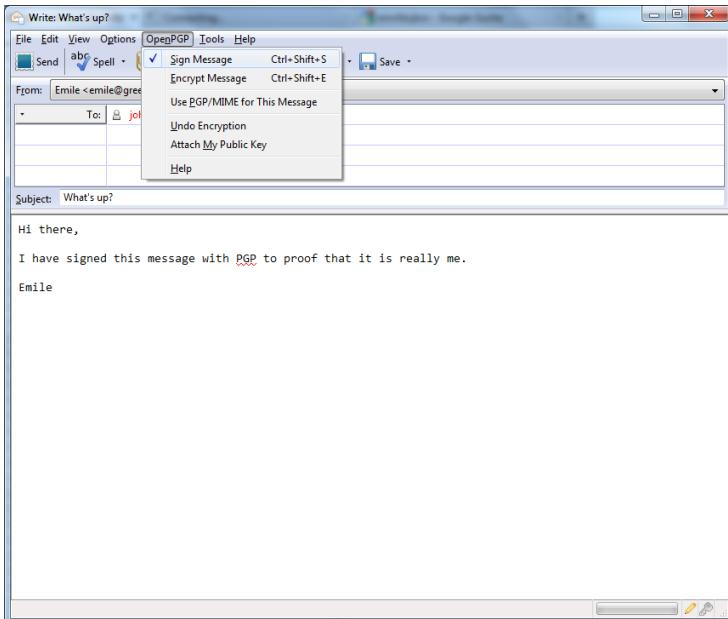


Figure 32.32: Ejemplo

- 
4. Pulse el botón *Send* y su mensaje firmado será enviado.

## Envío de mensajes cifrados a una destinatario en particular

1. Intercambie previamente claves públicas con sus amigos y colegas como explicamos anteriormente en este capítulo.
2. En Thunderbird, presione el ícono *Write*.
3. Redacte un mensaje a su amigo o colega, del cual haya recibido previamente su clave pública. **Recuerde que la línea del asunto del mensaje no será cifrada**, sólo se cifrará el cuerpo del mensaje y sus archivos adjuntos.
4. Antes de enviar el mensaje, habilite la opción **OpenPGP > Encrypt Message** en la barra de menú de la ventana de redacción del mensaje, si aún no está habilitada. Hecho esto, al pulsar sobre ella, aparecerá una firma marcada. Haciendo otro click debería deshabilitarse el cifrado. Observe el ejemplo más abajo.
5. Presione el botón *Send* para enviar su mensaje cifrado.

## Cifrado automático para destinatarios específicos

A menudo querrá asegurarse de que todos sus mensajes a un colega o amigo estén firmados y cifrados. Esta es una buena práctica, porque es posible que se olvide de habilitar el cifrado manualmente. Usted puede hacer esto mediante la modificación de las normas por receptores. Para ello accedamos al editor de reglas OpenPGP por destinatario.

## Creación de sus claves PGP

---

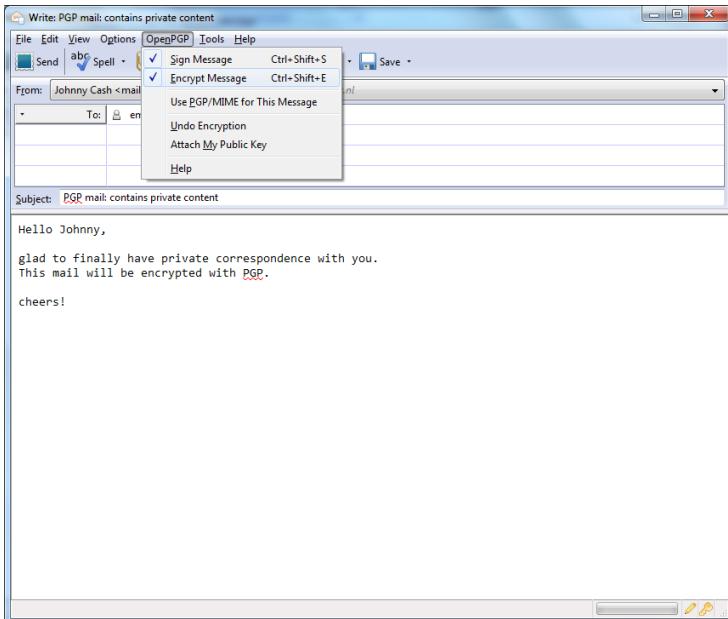


Figure 32.33: Cifrado del mensaje

---

Seleccione OpenPGP > Preferences desde la barra de menú de Thunderbird.

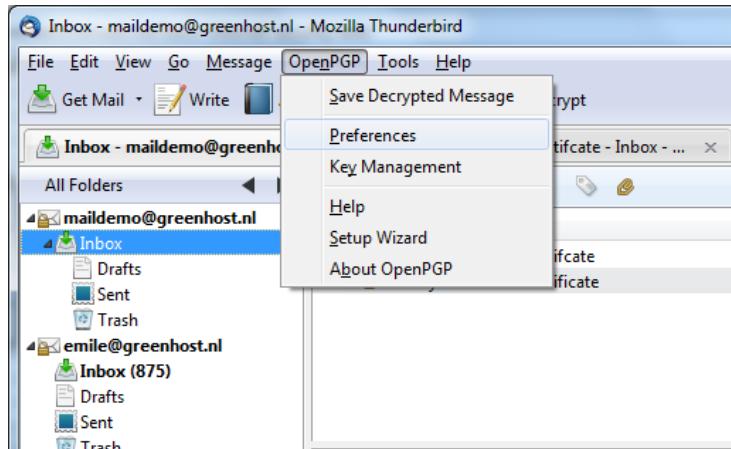


Figure 32.34: Editando reglas

la ventana de preferencias aparecerá. Pulse ‘Display Expert Settings’.

Aparecerán nuevas pestañas en la ventana. Vaya a la pestaña ‘Key Selection’ y haga click en el botón etiquetado como ‘Edit Rules ...’

Ahora veremos el editor de reglas por (ver más abajo). Este editor puede ser usado para especificar la forma en cómo los mensajes a ciertos destinatarios son enviados. Ahora vamos a agregar una regla que diga que queremos cifrar y firmar todos los mensajes de correo para `maildemo@greenhost.nl`

Primero haga click en el botón ‘Add’.

Aparecerá la ventana para añadir una nueva regla.

Lo primero que deberíamos ingresar es la dirección de correo

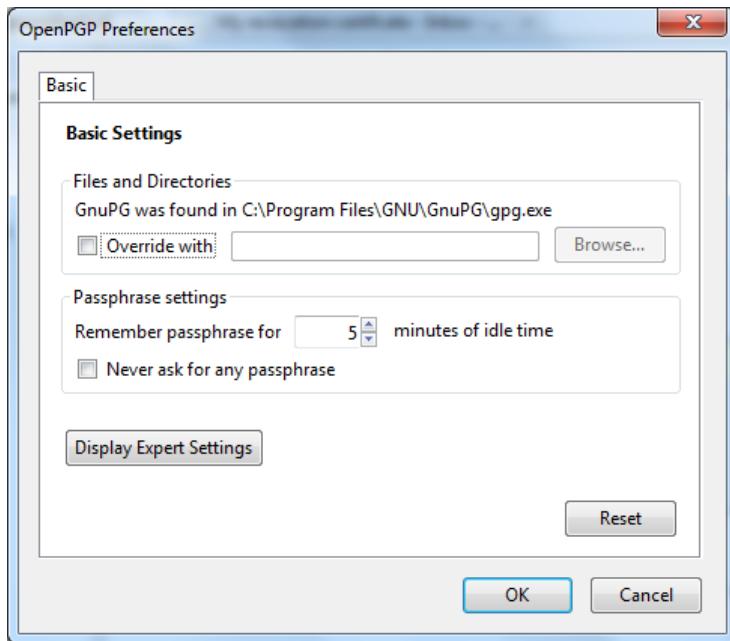


Figure 32.35: Preferencias

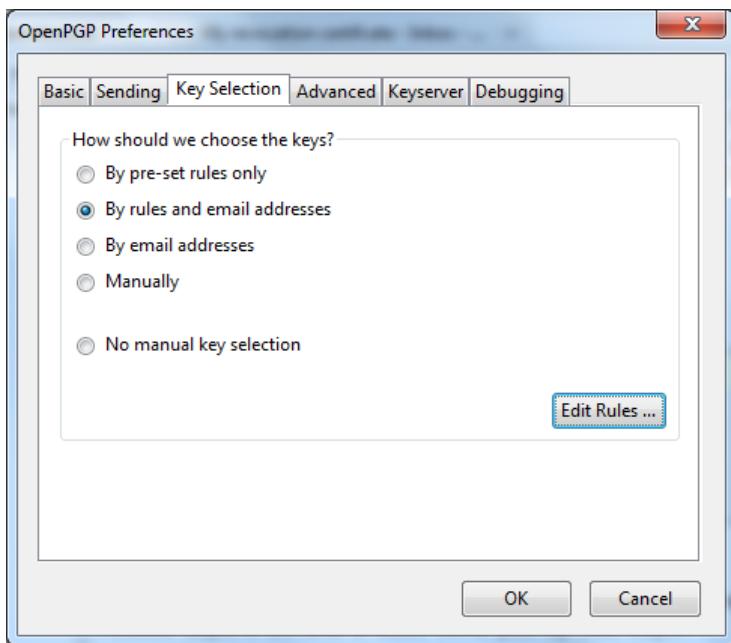


Figure 32.36: Selección y edición

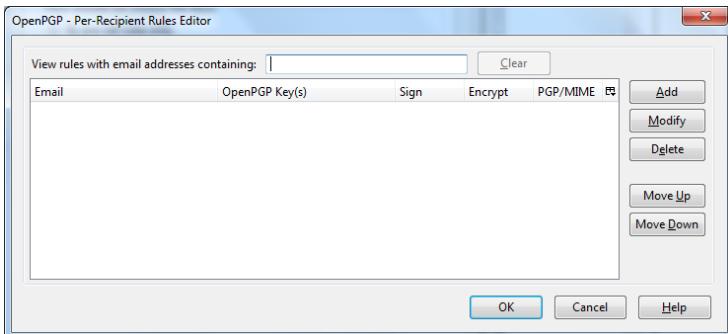


Figure 32.37: agregando...

electrónico del destinatario. En el ejemplo de más abajo, hemos ingresado `maildemo@greenhost.nl`

Ahora vamos a configurar los valores predeterminados de cifrado mediante el uso de los menús desplegables. Para firmar seleccione ‘Always’. Para cifrar seleccione ‘Always’.

Finalmente seleccionemos la *clave pública* del destinatario, con la cual cifaremos nuestro mensaje. No olvide este paso, es muy importante, de otra forma su mensaje no será cifrado. Pulse el botón etiquetado como ‘Select Key(s)...’. La ventana de selección de claves aparecerá. La clave más obvia se seleccionará por defecto. En el ejemplo debajo, solo hay disponible una única clave pública. Podemos seleccionar claves haciendo click sobre la pequeña casilla cercana a la dirección. Luego, presionando ‘OK’, cerramos todas las ventanas relevantes y habremos terminado.

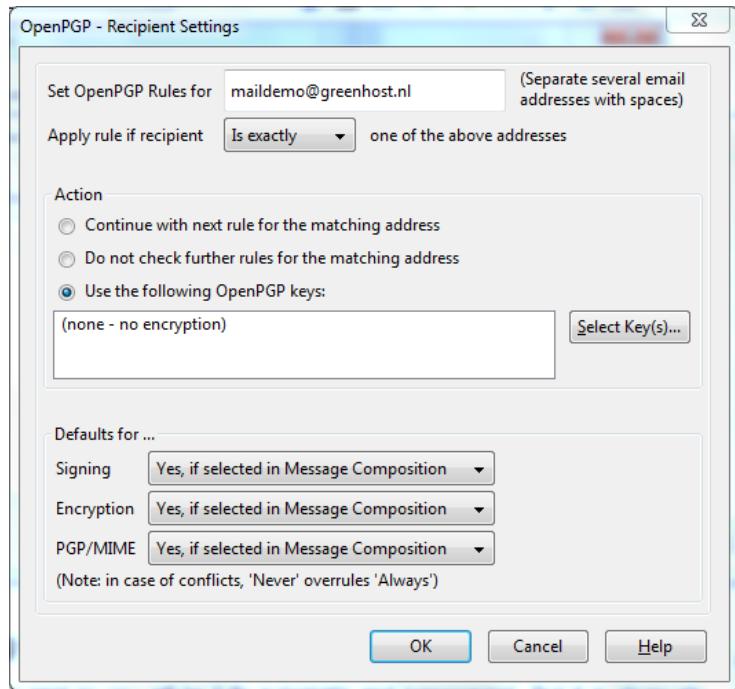


Figure 32.38: Ingresando la dirección de correo

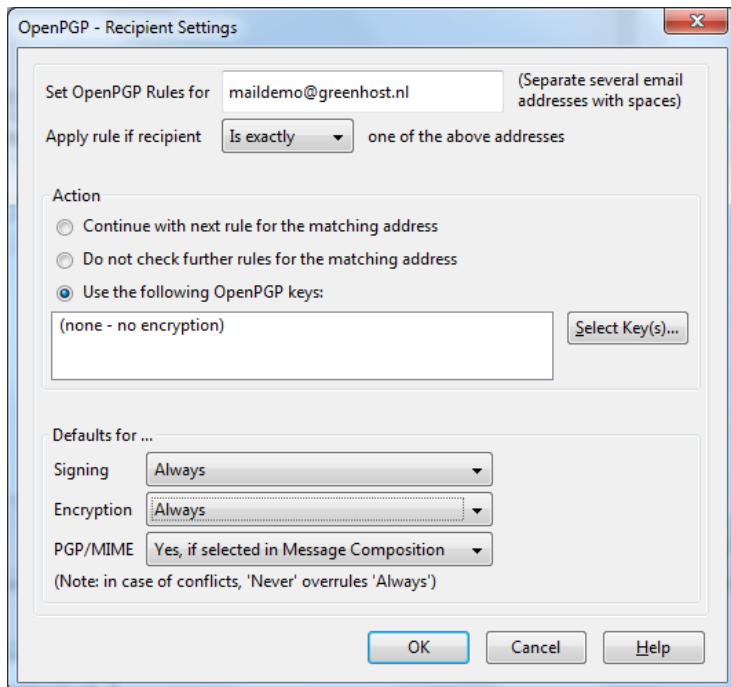


Figure 32.39: Configurndo...

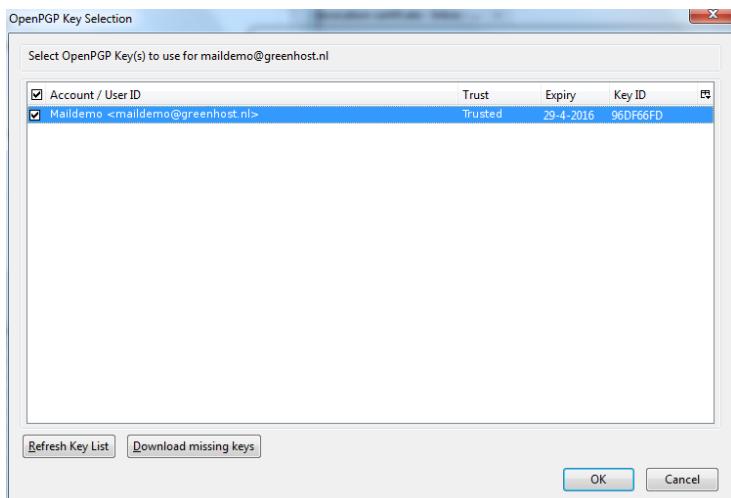


Figure 32.40: Finalizando....

## Verificación de mensajes entrantes

El descifrado de sus mensajes entrantes será automático y transparente. Pero es obvio que es muy importante que usted verifique que el mensaje estaba cifrado y/o firmado. Esta información está disponible en la barra especial sobre el cuerpo del mensaje.

Una firma válida será reconocida con una barra verde sobre el mensaje tal como se muestra la imagen debajo:

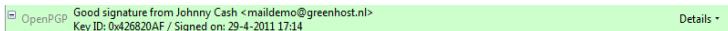


Figure 32.41: Firma válida

El último ejemplo estaba firmado pero no cifrado. Si el mensaje ha sido cifrado, lucirá algo así:



Figure 32.42: Mensaje cifrado

Cuando aparezca un mensaje que ha sido cifrado, pero sin firmar, puede resultar una falsificación hecha por alguien. La barra de estado se volverá gris, como en la imagen de abajo y le dirá que aunque el mensaje ha sido enviado de manera segura (cifrada), el remitente puede ser otro y no la persona detrás de la dirección de correo electrónico que se verá en el campo 'From'. La firma es necesaria para verificar el remitente real del mensaje. Por supuesto, es perfectamente posible que usted haya publicado su clave pública en Internet y permiten que las personas le envíen mensajes de correo electrónico anónimos. Pero también es posible que alguien está tratando de hacerse pasar por uno de sus amigos.

De forma similar, si usted recibe un mensaje firmado de alguien

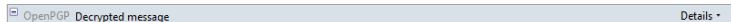


Figure 32.43: Mensaje cifrado sin firma

que conozca y posee su clave pública, pero la barra de estado se ha vuelto amarilla y muestra un mensaje de advertencia, es posible que alguien esté intentando enviarle correos electrónicos falsos.

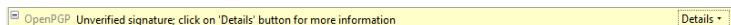


Figure 32.44: Advertencia

A veces las claves secretas son robadas o perdidas. El propietario de la clave deberá informar a sus amigos y enviarles un certificado de revocación (más explicación de esto en el siguiente párrafo). La revocación significa que ya no confía en la clave antigua. El ladrón podría probar suerte más tarde enviándole un mensaje de correo electrónico firmado falsamente. La barra de estado ahora se verá así:



Figure 32.45: Barra de estado

Curiosamente Thunderbird en esta situación ¡seguirá mostrando una barra de estado verde! Es importante tener en cuenta el contenido de la barra de estado con el fin de entender los aspectos de cifrado de un mensaje. GPG permite una gran seguridad y privacidad, pero sólo si está familiarizado con su uso y conceptos. Preste atención a las advertencias en la barra de estado.

## Revocación de su par de claves GPG

Su clave secreta ha sido robada por alguien. Su disco duro se rompió y ha perdido todos sus datos. Si la clave se pierde, ya no se pueden descifrar los mensajes. Si la clave ha sido robada, alguien puede descifrar su comunicación. Es necesario hacer un nuevo juego de claves. El proceso de creación de claves, utilizando el asistente OpenPGP en Thunderbird, ha sido descrita en este manual. Pero primero debe decirle al mundo que su clave pública vieja ya no tiene valor, e incluso es peligroso su uso.

## Qué hacer si pierde su clave secreta, u olvida la frase de paso

Durante la creación de su par de claves, el asistente OpenPGP le ofreció la posibilidad de crear un certificado de revocación. Este es un archivo especial que usted envíe a los demás para advertirles que hay que desactivar la clave. Si usted tiene una copia de este archivo, el envío de la clave de revocación es simplemente enviar el archivo como un archivo adjunto a todos sus amigos. Ya no puede enviar correos firmados (obviamente, porque ha perdido su clave secreta). Eso no tiene importancia. Envíelo como un correo normal. El certificado de revocación sólo pudo haber sido creado por el propietario de la clave secreta y prueba que él desea revocarla. Es por eso que normalmente debe mantenerse oculto a los demás.

Si usted no tiene el certificado de revocación, no existe otra opción que ponerse en contacto con sus amigos e informarles personalmente que su llave se ha perdido y que ya no deberían confiar en ella.

---

## **Qué hacer si robaron su clave secreta, o si la misma está comprometida**

Si tiene razones para sospechar que su clave secreta ha sido comprometida, o peor, su clave y contraseña, es muy importante ponerse en contacto con los demás para decirles que dejen de enviarle mensajes cifrados. Con su clave privada, otras personas serán capaces de romper el cifrado de los mensajes de correo electrónico si también tienen su frase de contraseña. Esto también es cierto para aquellos mensajes que ha enviado en el pasado. Descifrar la frase de paso no es sencillo, pero puede ser posible si la persona tiene muchos recursos, como un estado o una gran organización, por ejemplo, o si su contraseña es demasiado débil. En cualquier caso, debe asumir lo peor y asumir que la frase de contraseña puede haber sido comprometida. Envíe un archivo de revocación de certificados a todos tus amigos o póngase en contacto con ellos personalmente para informarles de la situación.

Incluso después de haber revocado su par de claves viejas, la clave robado todavía se puede utilizar para descifrar su correspondencia anterior. Usted debe considerar otras maneras de proteger la correspondencia antigua, por ejemplo, volver a cifrarla con una clave nueva. La última operación no se discutirá en este manual. Si no está seguro de cómo hacerlo, debe buscar la ayuda de expertos o más información en la web.

## **Recepción de un mensaje de revocación**

Si uno de sus amigos le envía a usted un certificado de revocación, le está pidiendo que desconfíe de su clave pública a partir de ahora. Usted siempre debe aceptar la solicitud y debe ‘importar’ el certificado para desactivar su clave. El proceso de

aceptación de un certificado de revocación es exactamente el mismo que aceptar una clave pública, como ya se ha descrito en el capítulo. Thunderbird le preguntará si desea importar el archivo ‘OpenPGP key’. Una vez que lo ha hecho, una ventana emergente de confirmación similar a la siguiente deberá aparecer.

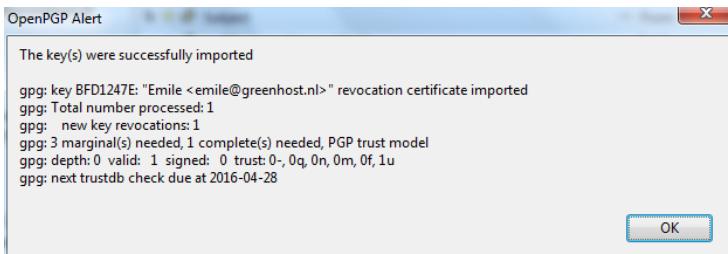


Figure 32.46: Aceptación de una revocación

## Preparándose para lo peor: copias de resguardo de sus claves

Sus claves son almacenados en el disco rígido como archivos normales. Pueden perderse si el equipo se daña. Se recomienda encarecidamente mantener una copia de seguridad de sus claves en un lugar seguro, como una caja fuerte. Hacer una copia de seguridad de su clave secreta tiene otra ventaja de seguridad también. Cada vez que usted teme que su computadora se encuentra en peligro inmediato de ser confiscada, puede eliminar el par de claves. Su correo electrónico será ilegible inmediatamente. En una etapa posterior, puede recuperar las claves de la bóveda y volver a importarlas en Thunderbird.

Para realizar una copia de seguridad de su par de claves, diríjase

---

al administrador de claves utilizando el menú de Thunderbird y haga clic en OpenPGP > Key Management.

Es necesario haber seleccionado la opción ‘Display All Keys by Default’ para obtener una lista de todas sus claves. Busque su propia dirección de correo en la lista y haga click con el botón derecho sobre ella. Una ventana de selección aparecerá con algunas opciones. Seleccione la opción ‘Export Keys to File’.

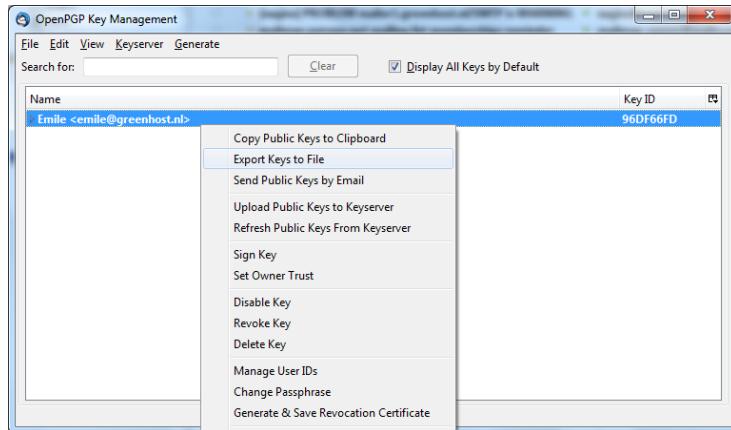


Figure 32.47: Copia de seguridad

Ahora deberá grabar el par de claves en un archivo. Thunderbird le preguntará si desea incluir la clave secreta. Si así lo desea, seleccione ‘Export Secret Keys’.

Finalmente Thunderbird le preguntará dónde almacenar el archivo de claves. Puede hacerlo donde más lo desee, disco de red, memoria USB, etc. Solo recuerde ocultarla de otras personas.



Figure 32.48: Exportando las claves

## Lecturas adicionales

Más documentación referida al uso de GPG con Thunderbird puede ser encontrada en el sitio web del plugin Enigmail. Consulte el manual de Enigmail

<http://enigmail.mozdev.org/documentation/handbook.php>.  
html Webmail y PGP =====

La única forma segura de cifrar el correo electrónico dentro de la ventana del navegador es cifrar el texto fuera de la ventana y luego copiarlo y pegarlo adentro.

Por ejemplo, escriba el texto en un editor de texto como gedit, kate o vim y guárdelo con extensión .txt (en este ejemplo “mensaje.txt”). A continuación, escriba

```
gpg -ase -r <dirección de email/gpg id> -r <gpg id> mensaje.txt
```

Un nuevo archivo llamado “mensaje.asc” se creará. Contiene el mensaje cifrado y por lo tanto ya puede adjuntarse en un correo electrónico o se puede copiar y pegar el contenido de forma segura en la ventana del navegador.

Para descifrar un mensaje desde la ventana del navegador, basta con escribir gpg en la línea de comandos y pulsar Enter. A continuación, copie y pegue el mensaje a descifrar en la ventana de línea de comandos y, después que le preguntan su contraseña, pulse Ctrl+D (esto añade un carácter de fin de archivo y le solicita a gpg el mensaje de texto descifrado).

---

Si utilizar la línea de comandos le parece demasiado complicado, podría considerar la posibilidad de instalar una aplicación de ayuda como gpgApplet, kgpg o cualquier otra aplicación que posea su sistema operativo. ¿Por qué usar Firefox?

=====

Firefox es software de código abierto desarrollado por una organización sin fines de lucro, la Fundación Mozilla. Por eso, es independiente de los intereses de cualquier empresa aunque un gran porcentaje de su financiación proviene de Google para poder colocar a su motor de búsqueda como la opción por defecto dentro del navegador web Firefox. Además, es altamente extensible a través de sus complementos y plugins, que le permiten al usuario mantener un mayor control acerca de cómo actúa el navegador comparado a Internet Explorer o Chrome (y a su versión de código abierto, Chromium). Sin embargo, debe señalarse que esta extensibilidad a través de sus complementos es un arma de doble filo ya que dichos complementos pueden subvertir el normal funcionamiento del navegador además de mejorararlo.

Si no está cómodo con Google como su motor de búsqueda por defecto, puede ser cambiado por medio de la opción ‘Manage Search Engines...’ del menú desplegable de la caja de búsqueda. Algunos de los motores de búsqueda pro-privacidad más recomendables son Startpage y DuckDuckGo.



# 33

## Accediendo a Firefox en Ubuntu

Firefox viene instalado en Ubuntu por defecto. Para abrirlo, haga click en el ícono de Firefox en la barra lateral de Unity:

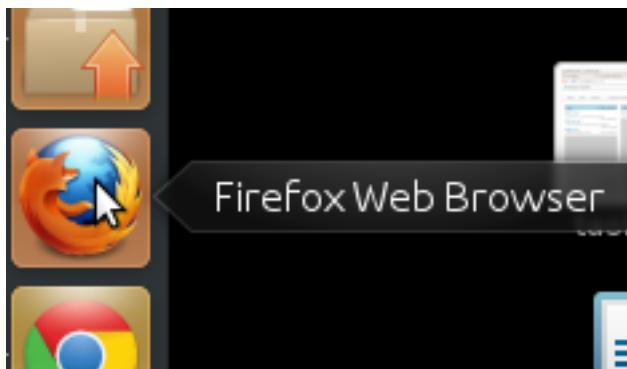


Figure 33.1: Abriendo Firefox

Firefox comienza abriendo una ventana de bienvenida:



Figure 33.2: Bienvenida

# 34

## Instalación en Mac OS X

1. Para descargar Firefox, visite su <https://www.mozilla.org/firefox> y haga click en el botón verde etiquetado como “Firefox Free Download”. La descarga debería comenzar automáticamente, si no es así, haga click en el enlace para descargarlo manualmente.
2. Cuando se lo pidan, haga click en **OK**.

Cuando se complete la descarga aparecerá una ventana similar a la siguiente:

3. Haga click y arrastre el ícono de **Firefox** sobre la parte superior del ícono de **Applications**.
4. Cuando la instalación haya terminado, cierre las dos ventanas pequeñas de Firefox.
5. Elimine la imagen de disco de Firefox. Si esto no funciona de forma normal, seleccione el ícono de imagen de disco y luego, en el menú Finder, seleccione **File > Eject Firefox**.
6. Ahora, abra el directorio **Applications** y arrastre el ícono de **Firefox** al dock:

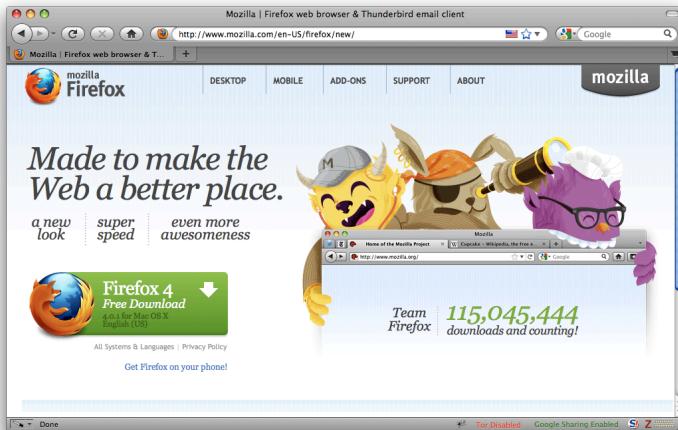


Figure 34.1: Descargando Firefox

7. Haga click en el ícono de **Firefox** en el Dock para ejecutarlo. Aparecerá la casilla de diálogos del asistente de importación:
8. Para importar sus marcadores, contraseñas y otros datos de Safari, haga click en **Continue**. Si no desea importar nada, solo seleccione **Cancel**.

Felicitaciones, ¡ya está preparado para usar Firefox!

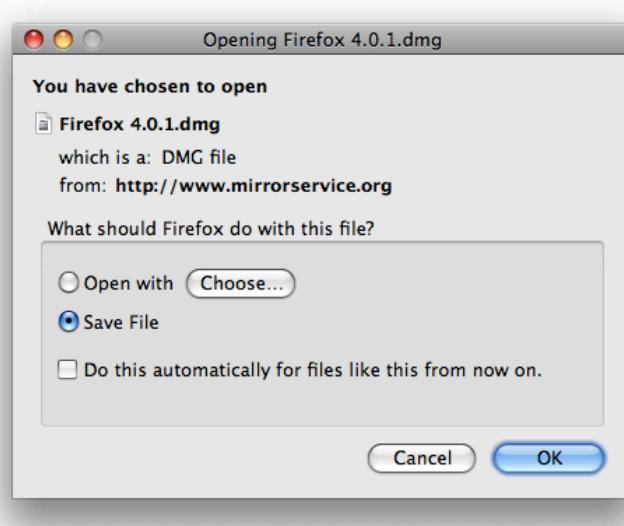


Figure 34.2: Inicio de descarga



Figure 34.3: Finalizando la descarga

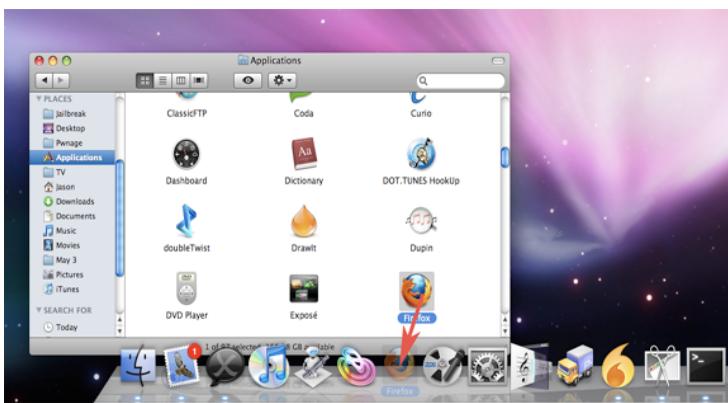


Figure 34.4: Poniendo el ícono en el dock

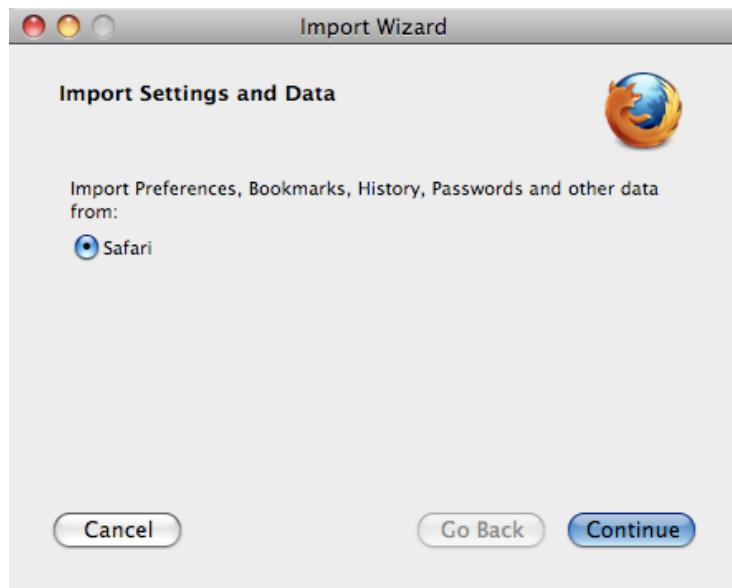


Figure 34.5: Asistente de importación

## Instalación en Mac OS X

---

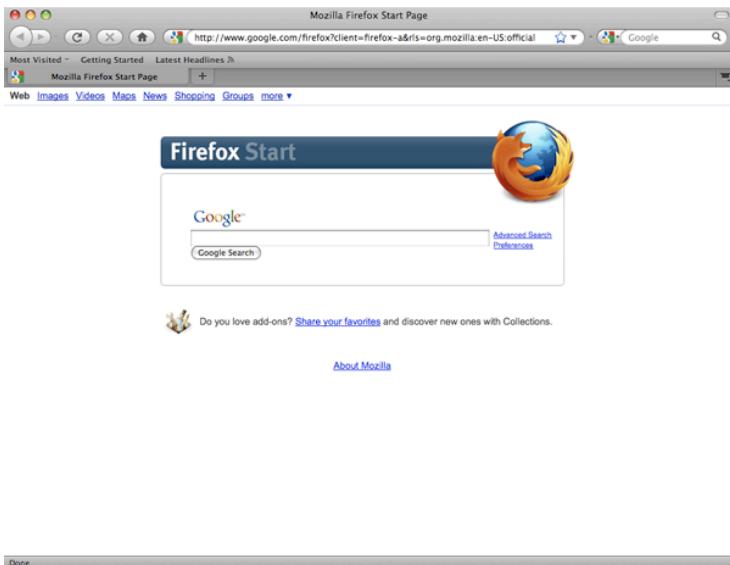


Figure 34.6: Instalación finalizada

# 35

## Instalación de Firefox en Windows

1. Para descargar Firefox, visite <https://www.mozilla.com/firefox/>.
2. Haga click en el botón de descarga y el archivo de instalación se descargará en su computadora.
3. Una vez completada la descarga, haga doble click en el archivo de instalación para iniciar el asistente.
  - Si está ejecutando Windows Vista, debería tener acceso al control de cuentas de usuario. En este caso, permita que se ejecute la configuración pulsando **Continue**.
  - Si está ejecutando Windows 7, se le preguntará si le permite a Firefox realizar cambios en su computadora. Haga click en **Yes**.

Aparecerá una pantalla de bienvenida.

4. Pulse **Next** para continuar. Se le preguntará si desea la instalación estándar, o si quieres personalizarla. Elija la

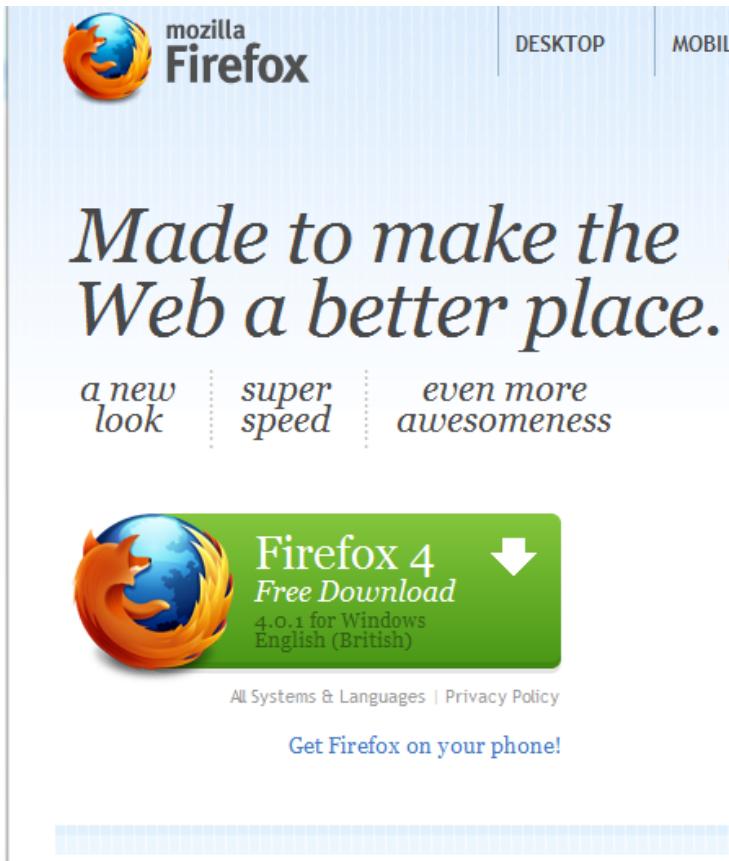


Figure 35.1: Descarga de Firefox

---

instalación estándar y haga click en **Next**.

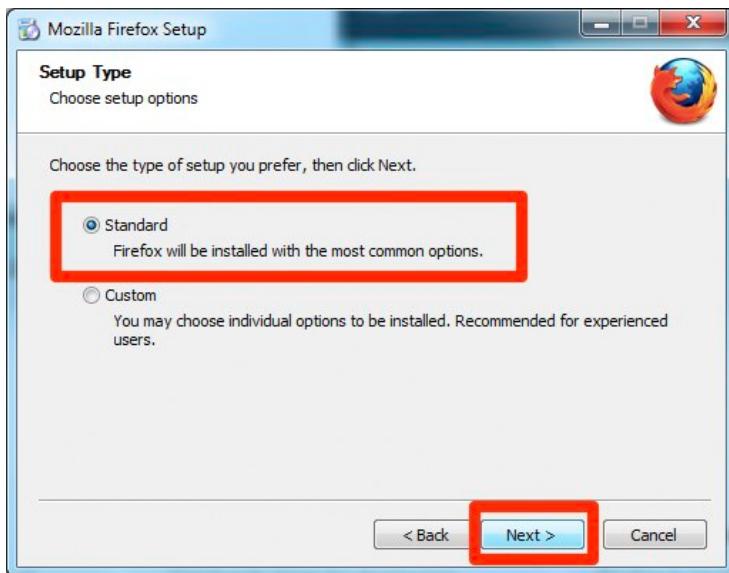


Figure 35.2: Instalación de Firefox

5. Se le preguntará si desea que Firefox sea su navegador por defecto. Se recomienda que sí lo sea.
6. Haga click en **Install**.
7. Para importar sus marcadores y otros datos de otros navegadores (por ejemplo Internet Explorer),haga click en **Continue**. Si no desea importar nada, solo seleccione **Cancel**.
8. Una vez instalado Firefox, haga click en **Finish** para cerrar el asistente de configuración.

Si tilda la casilla de verificación **Launch Firefox now**, Firefox

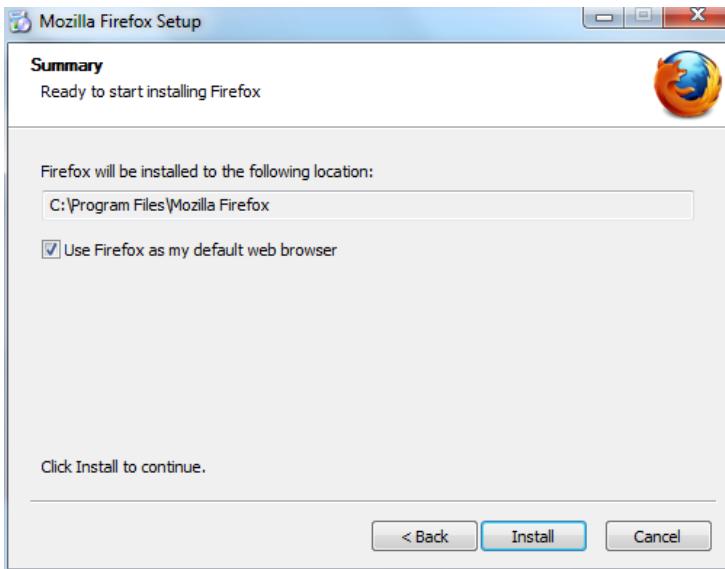


Figure 35.3: Windows Firefox Install

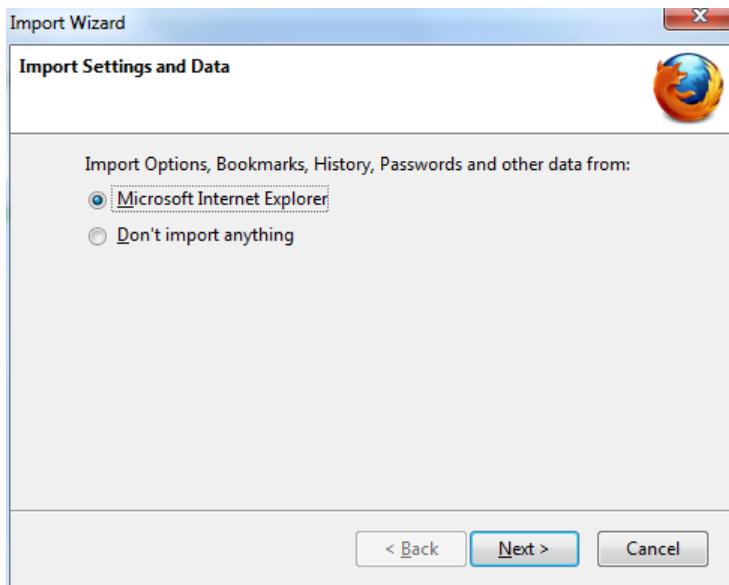


Figure 35.4: Importando marcadores

se ejecutará después que usted pulse **Finish**. Otra forma de ejecutarlo es a través del menú de inicio.

## Usuarios de Windows Vista

Si en ningún momento a través del proceso de instalación le piden ingresar con la ventana de control de cuenta de usuario, presione Continue, Allow, o Accept.

## Problemas

Si surgen problemas con el uso de Firefox, consulte <https://support.mozilla.com/kb/Firefox+will+not+start>

# 36

## Extensiones de Firefox

La primera vez que descargue e instale Firefox, puede manejar las tareas básicas del navegador inmediatamente. También puede agregar capacidades adicionales o cambiar la forma en que se comporta con la instalación de complementos, pequeños añadidos que extienden el poder de Firefox.

Las extensiones de Firefox optimizan su navegador, pero también pueden recoger y transmitir información sobre usted. Antes de instalar cualquier complemento, tenga en cuenta elegir los complementos a partir de fuentes confiables. De lo contrario, un complemento puede enviar información acerca de usted sin que usted lo sepa, mantener un registro de los sitios que ha visitado, o incluso dañar el equipo.

Hay varios tipos de complementos:

- *Extensiones* que agregan funcionalidad a Firefox.
- *Temas* que permiten cambiar la apariencia de Firefox.
- *Plugins* que ayudan a Firefox manejar las cosas que normalmente no puede procesar (por ejemplo, películas Flash, aplicaciones Java).

Para los temas que se tratan en este libro sólo vamos a necesitar

extensiones. Vamos a ver algunos complementos que son particularmente importantes para hacer frente a la seguridad en Internet. La variedad de extensiones disponibles es enorme. Puede añadir diccionarios de diferentes idiomas, realizar el seguimiento del clima en otros países, obtener sugerencias de los sitios web que son similares a la que usted está viendo en ese momento, y mucho más. Firefox mantiene una lista de las extensiones actuales disponibles en (<https://addons.mozilla.org/firefox>); también puede buscar por categoría en <https://addons.mozilla.org/firefox/browse>.

**Atención:** Nosotros le recomendamos que nunca instale un complemento si no está disponible en la página de complementos de Firefox. Usted nunca debe instalar Firefox a menos que obtenga los archivos de instalación de una fuente de confianza. Es importante tener en cuenta que el uso de Firefox en el ordenador de alguien o en un café con Internet aumenta su vulnerabilidad potencial. Sepa que usted puede tener Firefox en un CD o en una memoria USB (consulte el capítulo sobre este tema).

Si bien ningún instrumento puede protegerlo completamente contra todas las amenazas a su privacidad y seguridad en línea, las extensiones de Firefox que se describen en este capítulo pueden reducir significativamente su exposición a las más comunes, y aumentar sus posibilidades de permanecer en el anonimato.

## HTTPS Everywhere

HTTP es considerada insegura, porque la comunicación se transmite en texto plano. Muchos sitios en la Web ofrecen algún soporte para el cifrado HTTPS, pero es difícil de usar. Por ejemplo, pueden conectarse a HTTP de forma predeterminada, incluso cuando HTTPS está disponible, o pueden llenar las pági-

---

nas cifradas con vínculos que se remontan al sitio sin cifrar. La extensión HTTPS Everywhere soluciona estos problemas al volver a escribir todas las solicitudes a estos sitios a HTTPS. Aunque la extensión se llama “HTTPS Everywhere”, sólo se activa HTTPS en una lista particular de sitios y sólo pueden utilizar HTTPS en los sitios que han decidido apoyarlo. No se puede hacer la conexión a un sitio seguro si ese sitio no ofrece HTTPS como opción.

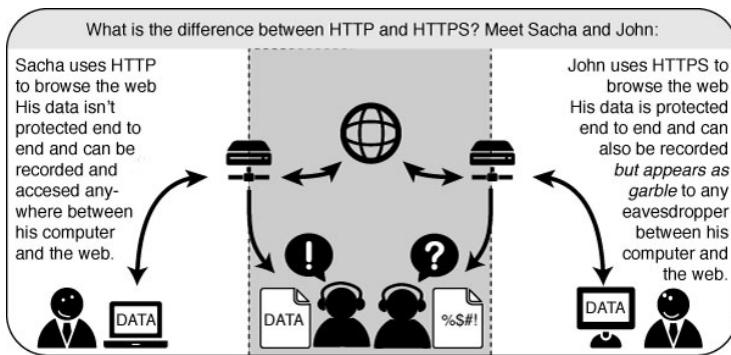


Figure 36.1: Esquema de HTTPS

Por favor, tenga en cuenta que algunos de estos sitios todavía incluyen una gran cantidad de contenido, como imágenes o íconos, de dominios de terceros que no están disponibles a través de HTTPS. Como siempre, si el ícono de la cerradura del navegador está roto o tiene un signo de exclamación, es posible que sigan siendo vulnerables a algunos adversarios que usan ataques activos o análisis de tráfico. Sin embargo, el esfuerzo que se requiere para controlar su navegación será mucho mayor.

Algunos sitios web (como Gmail) proporcionan soporte HTTPS automáticamente, pero utilizar HTTPS Everywhere también lo protegerá de ataques de eliminación de TLS/SSL, en los que un

atacante oculta la versión HTTPS del sitio desde su computadora si en un inicio se intenta acceder a la versión HTTP.

Información adicional se puede encontrar en su <https://www.eff.org/https-everywhere>.

## Instalación

Primero, descargue la extensión HTTPS Everywhere desde el sitio web oficial <https://www.eff.org/https-everywhere>



Figure 36.2: HTTPS Everywhere

Seleccione la versión más nueva. En el ejemplo debajo, usamos la versión 2.2 de HTTPS Everywhere. (Podría estar disponible una versión más nueva en este momento.)

Haga click en “Allow”. Tendrá que reiniciar Firefox pulsando el botón “Restart Now”. HTTPS Everywhere está instalado.



Figure 36.3: Seleccionando la versión más reciente

## Configuración

Para acceder al panel de configuración de HTTPS Everywhere en Firefox 4 (GNU/Linux), haga click en el menú Tools en la parte superior de su pantalla y luego seleccione complementos. (Observe que en diferentes versiones de Firefox y en diferentes sistemas operativos, el administrador de complementos puede estar en diferentes lugares en la interfaz.)



Figure 36.4: Configurando HTTPS Everywhere

Haga click en el botón Preferences.

Se mostrará una lista de todos los sitios web soportados donde las reglas de redirección de HTTPS pueden aplicarse. Si tiene problemas con una regla específica de redirección, puede desmarcarla aquí. En este caso, HTTPS Everywhere no modificará su

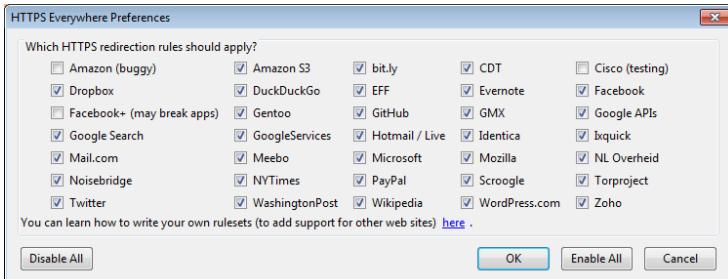


Figure 36.5: Preferencias

conexión con el sitio específico.

## Uso

Una vez habilitado y configurado, HTTPS Everywhere es muy fácil y transparente para usar. Tipee una URL como HTTP insegura (por ejemplo, `http://www.google.com`).

Presione Enter. Será redirigido automáticamente al sitio web seguro HTTPS cifrado (en este ejemplo: `https://encrypted.google.com`). No se necesita ninguna otra acción.

## Si las redes bloquean HTTPS

Su operador de red puede decidir bloquear las versiones seguras de los sitios web para aumentar su capacidad de espionar qué es lo que usted hace. En tales casos, HTTPS Everywhere puede advertirlo de usar estos sitios porque usted puede forzarlo para que nunca use las versiones inseguras. (Por ejemplo, sabemos

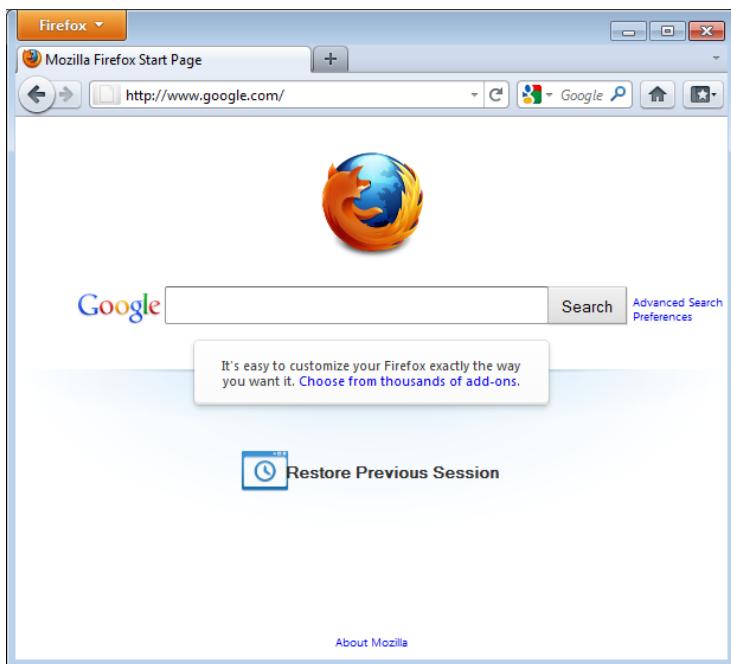


Figure 36.6: Usando HTTPS Everywhere

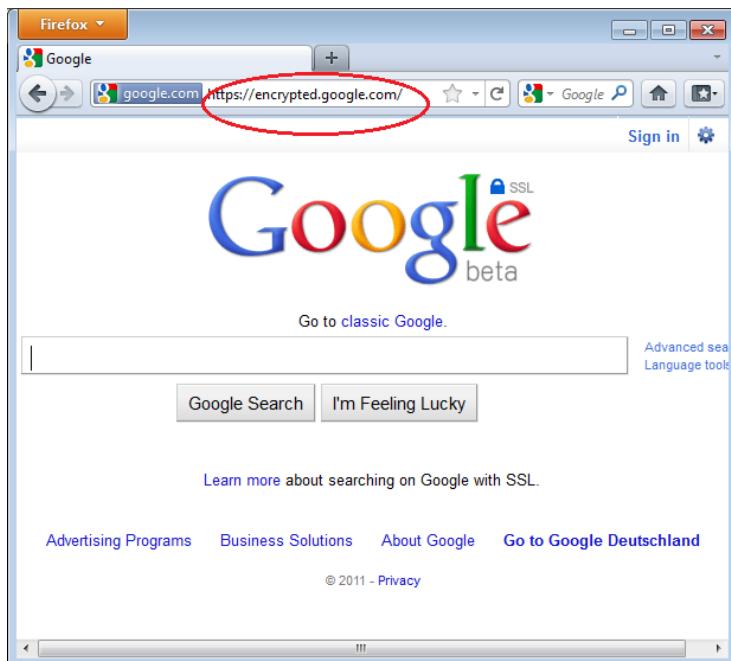


Figure 36.7: Redireccionamiento de HTTPS Everywhere

---

acerca de una red wifi de un aeropuerto donde todas las conexiones HTTP estaban permitidas, pero no las HTTPS. Quizás los operadores WiFi estaban interesados en ver que hacían los usuarios. En el aeropuerto, los usuarios con HTTPS Everywhere no podrán navegar por determinados sitios web a menos que deshabiliten temporalmente HTTPS Everywhere.)

En este escenario, usted debería elegir usar HTTPS Everywhere junto con una tecnología de evasión tal como Tor o una VPN para eludir a la red que está bloqueando el acceso seguro a los sitios web.

## Añadir soporte para sitios adicionales en HTTPS Everywhere

Usted puede agregar sus propias reglas a HTTPS Everywhere para sus sitios web favoritos. Puede encontrar cómo hacer esto en el siguiente <https://www.eff.org/https-everywhere/rulesets>. El beneficio de añadir reglas es que ellas le enseñan a HTTPS Everywhere cómo asegurarse que su acceso a estos sitios sea seguro. Pero recuerde: HTTPS Everywhere no le permitirá acceder a sitios seguros a menos que los operadores de los sitios hayan elegido ponerlos disponibles a través de HTTPS. Si un sitio no soporta HTTPS, no tendrá ningún beneficio añadir una regla para él.

Si usted administra un sitio web y dispone de una versión HTTPS del sitio disponible, una buena práctica sería la de presentar su sitio web al lanzamiento oficial de HTTPS Everywhere.

## Forzando conexiones seguras sobre servidor HTTPS

Aún cuando usted le de instrucciones a su navegador para que use el protocolo HTTPS cuando se comunique con un servidor web, es posible que el servidor (debido a una configuración insegura de su lado) fuerce a un protocolo cifrado SSL inseguro para la conexión. La única forma de prevenir es diciéndole al navegador que no acepte dichos protocolos inseguros SSL (como aquellos basados en cifrado RC4).

Para deshabilitar el cifrado RC4 para las conexiones HTTPS haga lo siguiente. En la barra de direcciones vacía tipee “about:config”, presione enter y cierre la ventana de diálogo de precaución que aparece (puede deshabilitar este diálogo si lo desea la próxima vez que configure Firefox). En el campo de búsqueda ingrese “rc4” y observe la lista desplegada como resultado de su búsqueda:

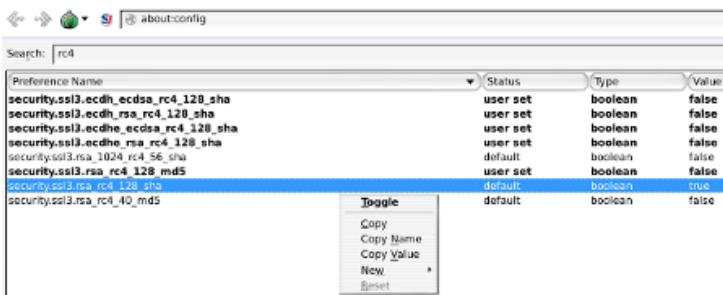


Figure 36.8: Deshabilitando RC4

Una entrada con un “true” en la última columna (campo “Value”) estará activa, debe desactivarla. Simplemente, con un click derecho en la entrada y cambie el valor a false. Proceda

---

de la misma forma para todas las entradas.

## Adblock Plus

Adblock Plus (<http://www.adblockplus.org>) es conocido principalmente por bloquear publicidad en los sitios web. Pero también se puede usar para bloquear otro contenido que intente rastrearlo. Para mantenerse actualizado con las últimas amenazas, Adblock Plus depende de las listas negras mantenidas por voluntarios.

Información extra para Geeks: ¿Cómo bloquea direcciones Adblock Plus?

El trabajo duro aquí está hecho realmente por Gecko, el motor sobre al cual se construyen aplicaciones tales como Firefox, Thunderbird y otros. Permiten lo se conoce como “políticas de contenido”. Una política de contenido no es más que un objeto JavaScript (o C++) que se llama cada vez que el navegador tiene que cargar algo. A continuación, puede ver la dirección que debe cargarse y algunos otros datos y decidir si se debe permitir o no. Existe una serie de directivas integradas de contenido (cuando usted define a qué sitios no se les debe permitir cargar las imágenes en Firefox o SeaMonkey, en realidad se está configurando una de estas políticas de contenido integrado) y ninguna extensión puede registrar alguna. Así que todo lo que Adblock Plus tiene que hacer es registrar su política de contenidos, aplicar una lógica para decidir qué direcciones bloquear e implementar la interfaz de usuario para permitir la configuración de los filtros.

## Comenzando con Adblock Plus

Una vez que está instalado Firefox:

1. Descargue la última versión de Adblock Plus desde la base de datos de los complementos de Firefox.
2. Confirme que quiere instalar Adblock haciendo click en “Install Now”.
3. Después que Adblock Plus se ha instalado, Firefox se reiniciará.

## Elección de una suscripción a un filtro

Adblock Plus por sí mismo no hace nada. Puede ver cada elemento que un sitio web intenta cargar, pero no sabe a cuál bloquear. Para eso están los filtros de Adblock's. Después de reiniciar Firefox, se le pedirá que elija una suscripción a un filtro (gratuita).

¿Cuál elegir? Adblock Plus ofrece algunos en un menú desplegable y posiblemente usted quiera saber algo acerca de las fortalezas y debilidades de cada uno. Un buen filtro para comenzar a proteger su privacidad es EasyList (también disponible en <http://easylist.adblockplus.org/en>).

Por muy tentador que pueda parecer, no se suscriba a demasiados filtros, ya que algunos pueden superponerse, lo que resulta en resultados inesperados. EasyList (principalmente dirigido a sitios en idioma inglés) funciona bien con otras extensiones EasyList (tales como extensiones específicas de la región, como las listas de RuAdList o listas temáticas como EasyPrivacy). Pero choca con la lista de Fanboy (otra lista con foco principal en sitios en idioma inglés).

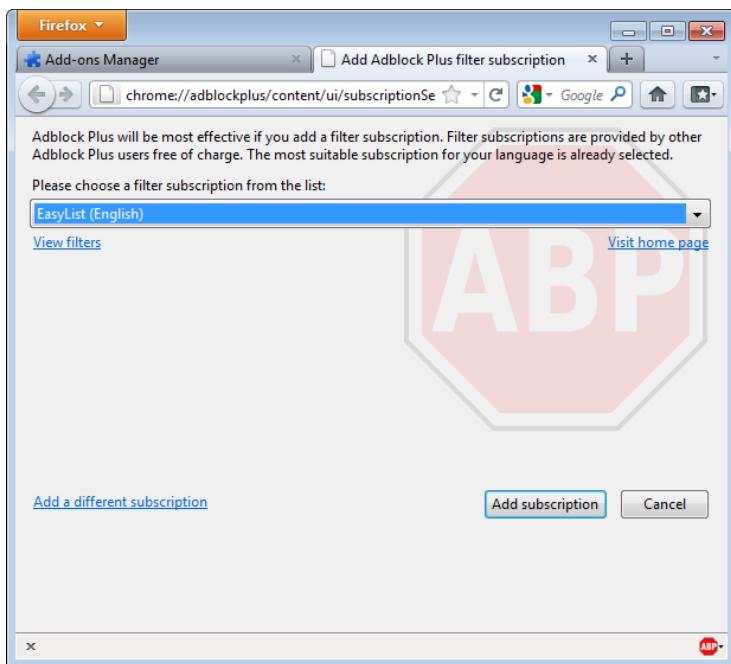


Figure 36.9: Ad Block Plus

Usted puede cambiar sus suscripciones de filtro en cualquier momento. Una vez hechos sus cambios, haga click en OK.

## Creación de filtros personalizados

AdBlock Plus también le permite crear sus propios filtros, si así lo desea. Para agregar un filtro, vaya a las preferencias de Ad-block Plus preferencias y haga clic en “Add Filter” en la esquina inferior izquierda de la ventana. Los filtros personalizados no pueden reemplazar los beneficios de las listas negras bien mantenidas como EasyList, pero son muy útiles para bloquear el contenido específico que no está cubierto en las listas públicas. Por ejemplo, si desea evitar la interacción con Facebook en otros sitios web, puede agregar el siguiente filtro:

```
||facebook.*$domain=~facebook.com|~127.0.0.1
```

La primera parte (||facebook.\*) bloqueará inicialmente todo lo que venga desde el dominio de Facebook. La segunda parte (\$domain=~facebook.com|~127.0.0.1) es una excepción que le dice al filtro que permita solicitudes de Facebook solamente cuando usted está en Facebook o si sus solicitudes de Facebook proceden desde 127.0.0.1 (su propia computadora) para mantener ciertas características de Facebook trabajando.

Puede encontrar una guía acerca de cómo crear sus propios filtros en <http://adblockplus.org/en/filters>.

---

## Habilitación y deshabilitación de Ad-Block Plus para elementos o sitios web específicos

Usted puede ver los elementos identificados por AdBlock Plus pulsando en el ícono ABP de AdBlock Plus en su navegador (habitualmente cerca de la barra de búsqueda) y seleccionar “Open blockable items”. Una ventana abajo en su navegador habilitará o deshabilitará cada elemento de la base caso por caso. Alternativamente, puede deshabilitar AdBlock Plus para un dominio o una página específica haciendo click en el ícono ABP y marcando la opción “Disable on [nombre del dominio]” o “Disable on this page only”.

## Otras extensiones que pueden mejorar su seguridad

Debajo hay una breve lista de extensiones que no están cubiertas en este libro y son de gran ayuda para su protección.

- **Flagfox** - pone una bandera en la barra de localización que le informa el lugar más probable en donde se encuentre el servidor web que hospeda la página web que está visitando <https://addons.mozilla.org/en-US/firefox/addon/flagfox/>
- **BetterPrivacy** - administra las “cookies” usadas para rastreaslo mientras visita sitios web. Las cookies son pequeñas cantidades de información almacenada en su navegador. Algunas de ellas son usadas por los publicistas para rastrear los sitios que usted visita. <https://addons.mozilla.org/en-US/firefox/addon/betterprivacy/>

- **GoogleSharing** - Si le preocupa que Google conozca su historial de búsqueda, esta extensión lo ayudará a evitarlo  
<https://addons.mozilla.org/en-US/firefox/addon/googlesharing/>
- **NoScript** - Aunque no es demasiado amigable para los principiantes, este complemento bloqueará los scripts y el contenido de los plugins de terceras partes (por ejemplo, Adobe Flash) a menos de que usted se lo permita específicamente, también brinda una protección general contra simples vectores de cross site scripting <http://noscript.net>
- **User Agent Switcher** - Su navegador envía gran cantidad de información a cualquier servidor remoto a través del encabezado ‘User-Agent’, incluyendo su sistema operativo e información específica sobre su versión. Este complemento le permite a usted falsificar dicha información o enviar un User-Agent genérico al servidor. <http://chrисpederick.com/work/user-agent-switcher/>

# 37

## Configuración de proxy

Un servidor proxy le permite a usted alcanzar un sitio web u otro lugar que esté bloqueado por su país o por su ISP. Existen muchas clases diferentes de proxies, que incluyen:

- Proxies web, que sólo requieren que usted conozca la dirección del sitio web del proxy. Una URL puede lucir así `http://www.example.com/cgi-bin/nph-proxy.cgi`
- HTTP proxies, que requieren que modifique la configuración de su navegador. Los proxies HTTP sólo trabajan en contenido web. Puede obtener más información acerca de un proxy HTTP en el formato `proxy.example.com:3128` o `192.168.0.1:8080`.
- Proxies SOCKS, que requieren modificar la configuración de su navegador. Los proxies SOCKS trabajan para muchas aplicaciones diferentes de Internet, incluso correo electrónico y herramientas de mensajería instantánea. La información sobre proxy SOCKS se parece a la información sobre proxy HTTP.

Usted puede usar un proxy web directamente sin ninguna configuración tipeando en la URL. Los proxies HTTP y SOCKS, sin embargo, tienen que configurarse en su navegador web.

## Configuración del proxy por defecto

En Firefox usted puede cambiar la configuración para usar un proxy. Necesitará abrir las opciones en la ventana de preferencias de Firefox. Puede encontrar esto en el menú, haciendo click en la parte superior y seleccionando **Edit > Preferences** en GNU/Linux o **Tools > Options** en Windows.

Vaya a la sección Network y abra la pestaña Advanced.

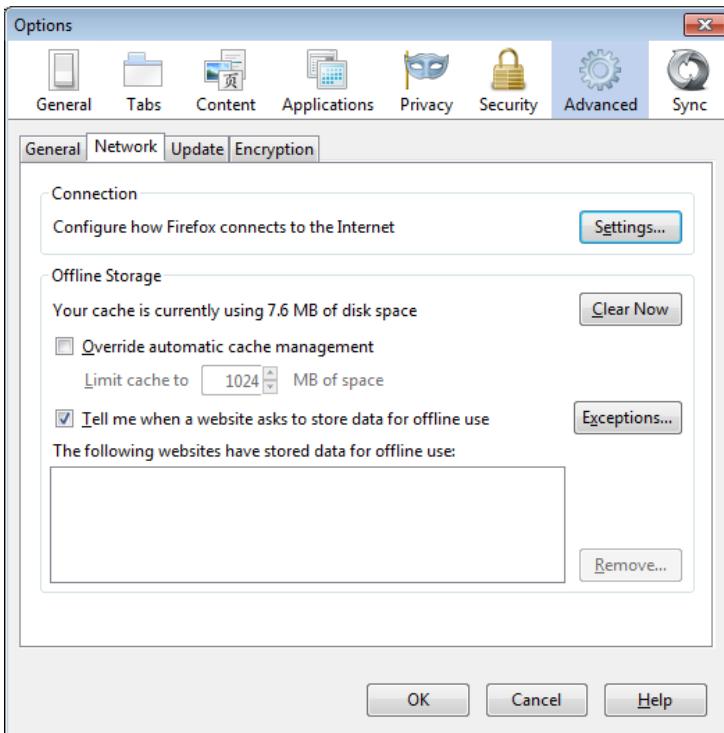


Figure 37.1: Configurando un proxy

---

Seleccione Settings, haga click en “Manual proxy configuration” e ingrese la información del servidor proxy que desea usar. Por favor recuerde que los proxies HTTP y los proxies SOCKS trabajan de distinta forma y tienen que ingresarse en sus correspondientes campos. Si hay dos puntos (:) en la información de su proxy, esto es una separación entre la dirección y el número de puerto. Su pantalla lucirá como esta:

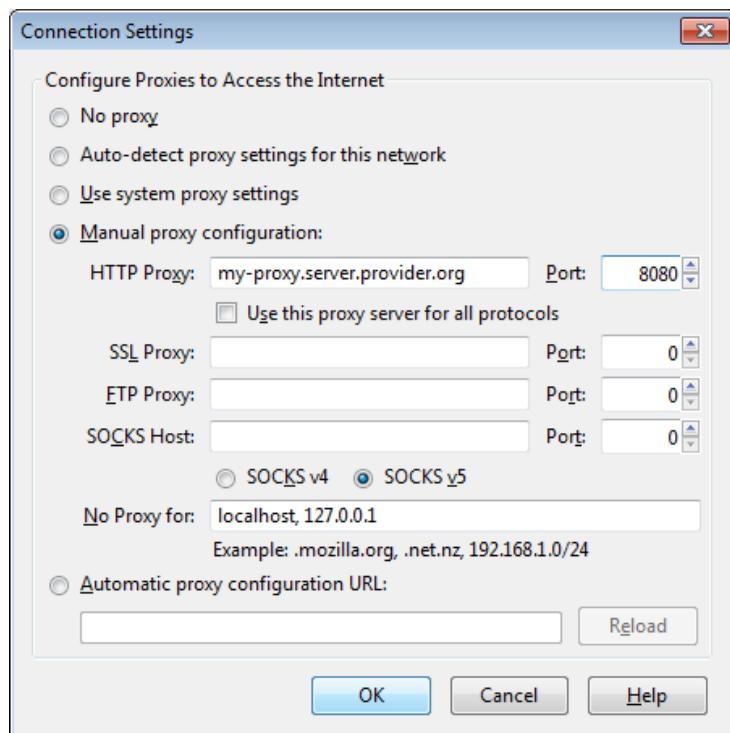


Figure 37.2: Proxy para Firefox

Después de hacer click en OK, su configuración será grabada

y su navegador web se conectará automáticamente a través del proxy en todas sus conexiones futuras. Si obtiene un mensaje de error tal como, “The proxy server is refusing connections” o “Unable to find the proxy server”, existe algún problema con su configuración del proxy. En este caso, repita los pasos anteriores y seleccione “No proxy” en la última pantalla para desactivar el proxy.

# 38

## Uso de Tor

Tor es un sistema pensado para facilitar el anonimato online, y está compuesto por un software cliente y una red de servidores los cuales pueden ocultar información acerca de la localización de los usuarios y otros factores que podrían identificarlos. Imagine un mensaje envuelto en muchas capas de protección: cada servidor tiene que quitar una capa, con lo que inmediatamente elimina la información del remitente del servidor anterior.

Si Alice desea visitar el sitio web de Bob en forma directa, lo representamos de la siguiente forma:

Alicia → Bob

Esto está bien, y Alicia y Bob podrán usar cifrado punto a punto para asegurarse la privacidad, la integridad y la autenticidad de sus comunicaciones. Sin embargo, si Alice no quiere que Bob sepa que ella está visitando su sitio web o no quiere que Eva (una hipotética espía, del lado de Alicia o del de Bob en la conexión) sepa que ella y Bob están comunicándose, se deben establecer algunos pasos extra.

Alicia debe entablar una conexión cifrada con un nodo de entrada de la red Tor, aquí se establecerá una conexión TLS y

el nodo de entrada le permitirá a Alicia establecer una comunicación a través de él. Una vez establecida dicha conexión TLS, se repite este proceso con un nodo de repetición, y entre éste y un nodo de salida. En este punto, Alicia cifrará sus datos 3 veces, primero a través del nodo de salida, luego a través del nodo repetidor y finalmente a través del nodo de entrada. La ruta establecida en la red luce de la siguiente manera:

**Alicia -> Nodo de entrada -> Nodo repetidor -> Nodo de salida -> Bob**

Cuando el nodo de entrada recibe los datos de Alicia estos están aún cifrados por el nodo repetidor y el nodo de salida. El nodo de entrada conoce su procedencia (Alicia) pero no su destino final (Bob) ni su contenido. El nodo repetidor recibe los datos del nodo de entrada y los trasmite al nodo de salida. Los datos aún están cifrados por el nodo de salida, y no conoce el origen (Alicia) ni el destino (Bob). Cuando el nodo de salida recibe los datos del nodo repetidor, se remueve la última capa de cifrado: el nodo de salida puede ver los datos y el destino (Bob) pero no conoce su origen (Alicia).

Esta aproximación por capas da su nombre a Tor (The Onion Router, el enrutador cebolla), cada capa conoce la capa en contacto con ella, y significa que nadie en la cadena excepto Alicia conoce la ruta completa que los datos están siguiendo; sin embargo, Alicia, Bob y el nodo de salida son capaces de leer el contenido del mensaje, por eso el cifrado punto a punto es requerido para asegurar la privacidad, la integridad y la autenticidad de las comunicaciones a través de la red Tor.

El uso de este sistema hace que sea más difícil de rastrear el tráfico de Internet del usuario, que incluye visitas a sitios web, publicaciones en línea, mensajes instantáneos y otras formas de comunicación. Su objetivo es proteger la libertad personal de los usuarios, la privacidad y capacidad de hacer negocios confidenciales, al mantener sus actividades en Internet a salvo del monitoreo. Tor es software libre y la red es de uso gratuito.

---

Como todas las redes actuales de anonimato de baja latencia, Tor no puede y no trata de protegerlo contra la vigilancia del tráfico en los extremos de la red, es decir, el tráfico que entra y sale de la red. Mientras que Tor proporciona protección contra el análisis de tráfico, no puede evitar la confirmación del tráfico (también llamada correlación de extremo a extremo)

Precaución: Como Tor no lo hace, y por diseño, no puede, cifrar el tráfico entre un nodo de salida y el servidor de destino, cualquier nodo de salida está en disposición de capturar cualquier tráfico que pasa a través de él, que no utilice cifrado de extremo a extremo, tal como TLS. (Si el cartero es corrupto, podría abrir el sobre y leer el contenido). Si bien esto puede o no violar el anonimato de la fuente, si los usuarios de Tor no cifran la comunicación de extremo a extremo ellos puede estar sujeto a un riesgo adicional de la interceptación de datos por parte de terceros. Resumiendo: la ubicación del usuario permanece oculta, sin embargo, en algunos casos el contenido es vulnerable al análisis a través del cual también se puede obtener información sobre el usuario.

## **Uso del paquete Tor para navegadores**

El paquete Tor para navegadores le permite usar Tor en Windows, OSX o GNU/Linux sin necesidad de configurar al navegador web. Aún mejor, también es una aplicación portable que se puede ejecutar desde una unidad flash USB, lo que le permite llevarlo a cualquier PC sin necesidad de instalarlo en el disco rígido de cada computadora.

## Descarga del paquete Tor para navegadores

Puede descargarlo desde el sitio web de torproject.org (<https://www.torproject.org>).

Si su país restringe el acceso al sitio web de tor, tipee “tor mirrors” en su motor de búsqueda web favorito: el resultado probablemente incluya algunas direcciones alternativas para descargarlo.

Por favor, siga las instrucciones del sitio web del proyecto Tor acerca de cómo instalarlo.

Precaución: cuando usted descarga el paquete Tor (en sus versiones completa o dividida), debería verificar las firmas de los archivos, especialmente si lo está descargando desde un sitio espejo. Este paso le asegura que los archivos no han sido falsificados. Para aprender más acerca de archivos de firma y cómo revisarlos, consulte <https://www.torproject.org/docs/verifying-signatures>

## Ejecutando un repetidor o un puente

Tor es una red de voluntarios que ejecutan repetidores y puentes. Si desea ayudar al crecimiento de la red Tor contribuyendo con ancho de banda y ciclos extra de CPU, considere ejecutar un repetidor. Además, al correr un repetidor puede mejorar su anonimato ya que un atacante no puede distinguir entre el tráfico originado por usted o por el repetidor. Consulte <https://www.torproject.org/docs/faq.html.en#BetterAnonymity> para obtener más detalles.

Sin embargo, si usted corre un repetidor, su dirección IP será listada en Internet como un repetidor Tor. Los clientes Tor

---

dependen de esta lista, provista por los servidores del directorio de Tor, para poder establecer los circuitos. Si desea contribuir con Tor, pero no desea correr un repetidor público, considere ejecutar un puente. Ya que los repetidores Tor son públicos, algunos ISP bloquean el acceso a la red Tor bloqueando *todos los repetidores*. Los puentes Tor, sin embargo, no están listados y además, son más difíciles de hallar.

La meta de Tor es proteger el anonimato en Internet, pero algunas veces se usa con fines ilegales. Como operador de un repetidor, consulte <https://www.torproject.org/eff/tor-legal-faq.html>, escrito por la Electronic Frontier Foundation (EFF). La EFF es una organización sin fines de lucro de EE.UU. cuya misión es “proteger sus derechos digitales.” En otros países, deberían buscar asesoramiento de organizaciones similares. Sin embargo, los riesgos legales pueden ser minimizados corriendo un repetidor que no sea de salida o un puente.

Si desea configurar su computadora para correr un repetidor o un puente, visite el <https://www.torproject.org/docs/tor-doc-relay.html.en> para obtener instrucciones. Extendiendo Google Chrome =====

Chrome es el navegador de Google. Aquí daremos algunos consejos y extensiones:

## Deshabilitación de búsqueda instantánea

Chrome puede buscar por tipo. La ventaja de esto es que usted puede recibir sugerencias de búsqueda y usar las predicciones de Google - pero las desventajas son que cada carácter que usted tipee puede ser enviado a los servidores de Google, donde queda

registrado.

Para deshabilitarlo, abra la configuración de Chrome haciendo click en el botón del menú a la derecha la barra de direcciones y pulsando Settings. O, simplemente tipee `chrome://settings/` en su barra de direcciones.

Asegúrese de la casilla de verificación **Enable Instant for faster searching (omnibox input may be logged)** esté desmarcada.

## AdBlock para Chrome

Como en Firefox, AdBlock remueve la publicidad. Puede instalarlo a partir de la página de Chrome Webstore.

## HTTPS Everywhere

Fuerza conexiones cifradas https donde sean posibles. El enlace de instalación puede encontrarse en su página web.

## PrivacyFix

PrivacyFix (beta) le proporciona la vista de tablero de mandos de la configuración de su privacidad en Facebook y Google, así como los encabezados de Do-Not-Track y las cookies de rastreo. Esto proporciona enlaces para cambiar rápidamente estos ajustes de privacidad sin excavar a través de muchas páginas de desglose. Se puede instalar desde la página de Chrome web store

# 39

## Manteniendo contraseñas seguras

Las contraseñas son como las llaves del mundo físico. Si pierde una contraseña no será capaz de entrar, y si los demás la copian o roban la podrán utilizar para entrar. Una buena contraseña no debe ser fácil de adivinar para los demás ni fácil de romper con las computadoras, sin dejar de ser fácil de recordar.

### **Extensión y complejidad de la contraseña**

Para evitar que sus contraseñas sean adivinadas, la longitud y complejidad son importantes. Las contraseñas como el nombre de su mascota o la fecha de nacimiento son muy inseguras, ya que utiliza una sola palabra que se puede encontrar en un diccionario. No utilice una contraseña que contenga solamente números. Lo más importante en una contraseña segura es que sea larga. El uso de combinaciones de letras minúsculas, mayúsculas, números y caracteres especiales pueden mejorar la seguridad, pero la longitud sigue siendo el factor más importante.

Utilice contraseñas de 20 caracteres por lo menos (cuanto más caracteres tenga, mejor) para asegurar cuentas importantes, como la frase de paso que protege su PGP/GPG o sus datos cifrados TrueCrypt, o la contraseña de su cuenta de correo electrónico principal . Ver [esta caricatura XKCD] (<https://xkcd.com/936/>) "correct horse battery staple" vis-à-vis "Tr0ub4dor&3" para obtener una explicación.

## Contraseñas seguras y fáciles de recordar

Una forma de crear una contraseña fuerte y fácil de recordar es usar frases.

Unos pocos ejemplos:

- ‘AmoAdouglasAdamsPorqueEsRealmenteGenial. ’
- ‘LaGenteAmaAlasMaquinasEnEl2029. ’
- ‘BarneyDejComoConociAtuMadreEsImpresionante! ’

Las frases son fáciles de recordar, incluso si son 50 caracteres y contiene caracteres en mayúsculas, en minúsculas, símbolos y números.

## Minimizar los daños

Es importante minimizar el daño si uno de sus contraseñas está siempre en peligro. Utilice diferentes contraseñas para diferentes sitios web o cuentas, de esa manera que si una se ve comprometida, los demás no lo estarán. Cambie sus contraseñas de vez en cuando, especialmente si hay cuentas que consideran sensibles. De esta manera usted puede bloquear el acceso a un atacante que puede haber aprendido su antigua contraseña.

---

## El uso de un gestor de contraseñas

Recordar un montón de contraseñas diferentes puede ser difícil. Una solución es utilizar una aplicación dedicada a gestionar la mayor parte de sus contraseñas. La siguiente sección de este capítulo discutiremos *Keepass*, un gestor de contraseñas libre sin vulnerabilidades conocidas, siempre y cuando elijas una “contraseña maestra” suficientemente largo y compleja para asegurarlo.

Para guardar contraseñas de sitios web sólo, otra opción es el administrador de contraseñas integrado del navegador Firefox. ¡Asegúrese de establecer una contraseña maestra, de lo contrario esto es muy inseguro!

## La protección física

Cuando se utiliza un equipo público, como en una biblioteca, un cibercafé o cualquier equipo que no es de su propiedad, existen varios peligros. Usando el método de la vigilancia “sobre el hombro” alguien, posiblemente con una cámara, puede ver sus acciones y puede ver la cuenta con la que inicia sesión y la contraseña que escribe. Una amenaza menos evidente son los programas de software o dispositivos de hardware llamados “keyloggers”, que registran lo que escribe. Ellos pueden estar ocultos dentro de una computadora o un teclado y no verse fácilmente. No utilice computadoras públicas para iniciar sesión en sus cuentas privadas, tales como el correo electrónico. Si lo hace, cambie sus contraseñas tan pronto como vuelva a una computadora que posee y en la cual confíe.

## Otras advertencias

Algunas aplicaciones, como programas de chat o de correo electrónico puede pedirle guardar o “recordar” su nombre de usuario y contraseña, por lo que no tendrá que introducirlas cada vez que se abre el programa. Si lo hace, puede significar que su contraseña puede ser recuperada por otros programas que se ejecutan en la máquina, o directamente desde el disco duro por alguien con acceso físico a la misma.

Si la información de inicio de sesión se envía a través de una conexión o canal inseguro, podría caer en las manos equivocadas. Consulte los capítulos sobre la navegación segura para más información. Instalación de KeePass

---

Explicaremos la instalación de KeePass en Ubuntu, en Windows y en Mac OSX.

Mac OS X viene con un excelente archivo administrador integrado de contraseña llamada Keychain que es bastante seguro. Los inconvenientes son que no es de código abierto y no funciona en otros sistemas operativos. Si lo necesitas para llevar tus contraseñas de un sistema operativo a otro, es mejor quedarse con Keepass después de todo. Cómo utilizar Keychain se explicará en el capítulo siguiente.

## Instalación de KeePassX en Ubuntu

Para instalarlo en Ubuntu vamos a utilizar el Ubuntu Software Center. Escriba KeePass en el campo de búsqueda en la parte superior derecha y la aplicación KeePassX deberá aparecer automáticamente en el listado.

Resalte el elemento (que puede estar ya resaltado por defecto)

---

y pulse en “Instalar”. Se le pedirá autorización para el proceso de instalación:



Figure 39.1: Instalación de KeePass

Introduzca la contraseña y pulse «verificar», el proceso de instalación comenzará entonces.

Ubuntu no ofrece una respuesta muy buena para mostrar que el software está instalado. Si el indicador de progreso verde en la izquierda ha desaparecido y la barra de progreso de la derecha se ha ido entonces se puede suponer que el software está instalado.

## Instalación de KeePass en Windows

Primero visite la página web de descarga de KeePass y seleccione el instalador apropiado. En este capítulo se utiliza el Instalador actual.

Descárguelo a su computadora y haga doble click en el instalador. Primero se le pedirá que seleccione un idioma, vamos a

elegir el idioma Inglés:



Figure 39.2: Seleccionando el idioma de KeePass

Presione 'OK' y se mostrará la siguiente pantalla:

Sólo pulse en 'Next>' y vaya a la siguiente pantalla:

En la pantalla que se muestra arriba hay que seleccionar “Acepto el acuerdo” de lo contrario no podrá instalar el software. Elija esta opción y luego pulse ‘Next>’. En la siguiente pantalla se le pedirá determinar la ubicación de la instalación. Puede dejar los valores por defecto a menos que tenga una buena razón para cambiarlos.

Haga clic en ‘Next>’ y continúe.

La imagen de arriba muestra los componentes de KeePass que usted puede elegir. Deje los valores por defecto como están y pulse ‘Next>’. Llegará a una nueva pantalla:

Esto no hace otra cosa que mostrarle un resumen de sus opciones. Presione “Instalar” y el proceso de instalación comenzará.



Figure 39.3: Ventana de instalación

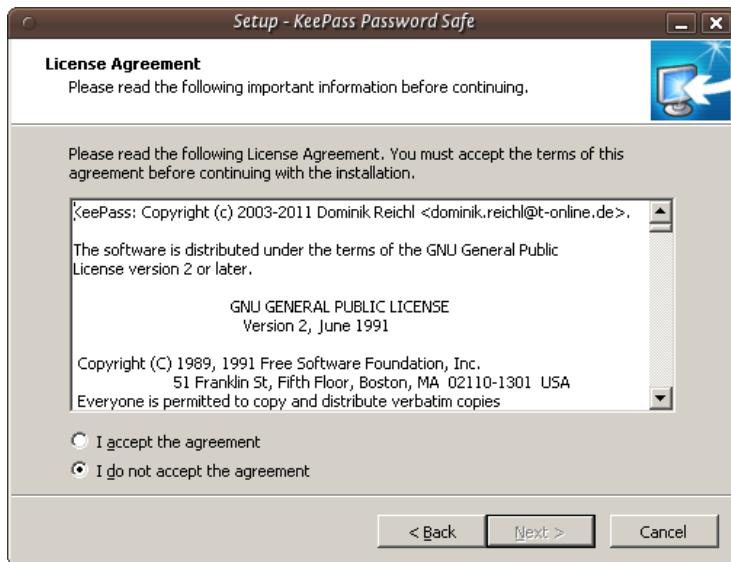


Figure 39.4: Pantalla de acuerdo

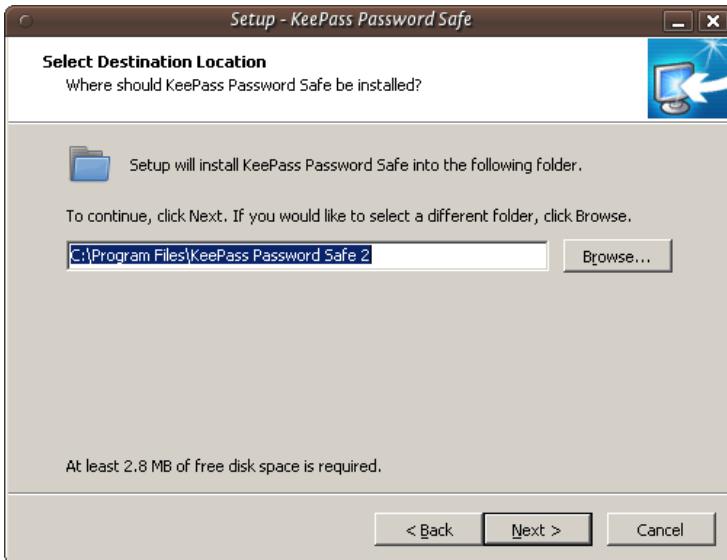


Figure 39.5: Configurando la ruta de instalación

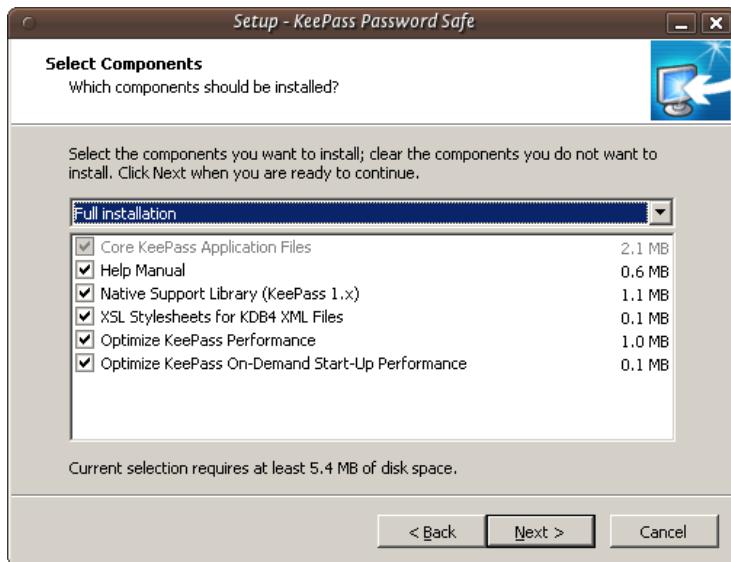


Figure 39.6: Keepass Install



Figure 39.7: Instalando Keepass

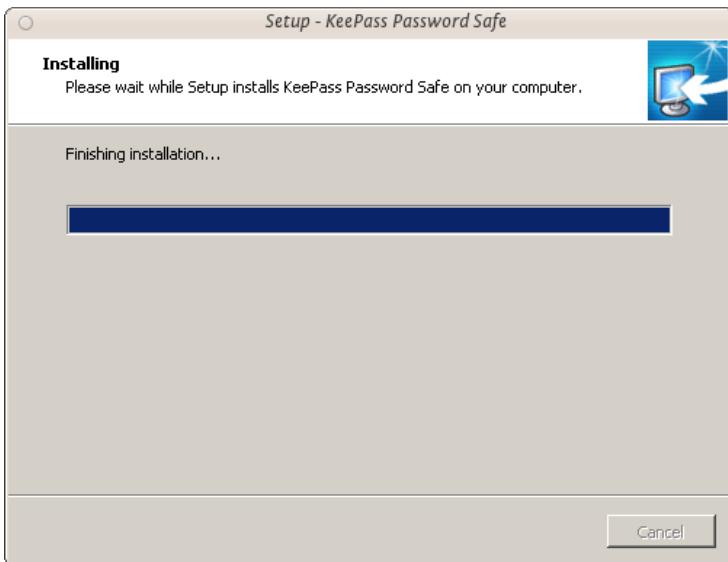


Figure 39.8: Confirmación de las opciones

---

## Instalación de KeePass en Mac OS X

Aunque KeyChain de Mac OS X hace un trabajo excelente al almacenar sus contraseñas, es posible que desee ejecutar su propia base datos y administrador de contraseñas. KeePass permite esta flexibilidad adicional. Primero visite la página web de descarga KeePass <http://keepass.info/download.html> y seleccione el instalador apropiado. Aunque los instaladores oficiales se enumeran en la parte superior de la página, hay instaladores no oficiales/contribuidos más abajo. Desplácese hacia abajo para encontrar [KeePass 2.x para Mac OS X][<http://keepass2.openix.be/>](<http://keepass2.openix.be/>):



Figure 39.9: Keepass para Mac OS X

Como se trata de un enlace externo, su navegador será redirigido a <http://keepass2.openix.be/>:



Figure 39.10: Redirección del navegador

Nótese aquí que debe instalar el framework Mono primero, para que KeePass puede ejecutarlo en Mac OS X. Haga un click sobre cada uno de los enlaces Mono 2.10.5 y KeePass2.18 para descargar los archivos DMG a su computadora. Haga doble click en cada uno de los DMGS en tus carpetas de descargas para descomprimir los volúmenes en el escritorio.

El programa de instalación del paquete Mono se llama ‘MonoFramework-MRE-2.10.5\_0.macos10.xamarin.x86.pkg’, por lo que debe hacer doble click en este documento en el volumen MonoFramework en el escritorio:

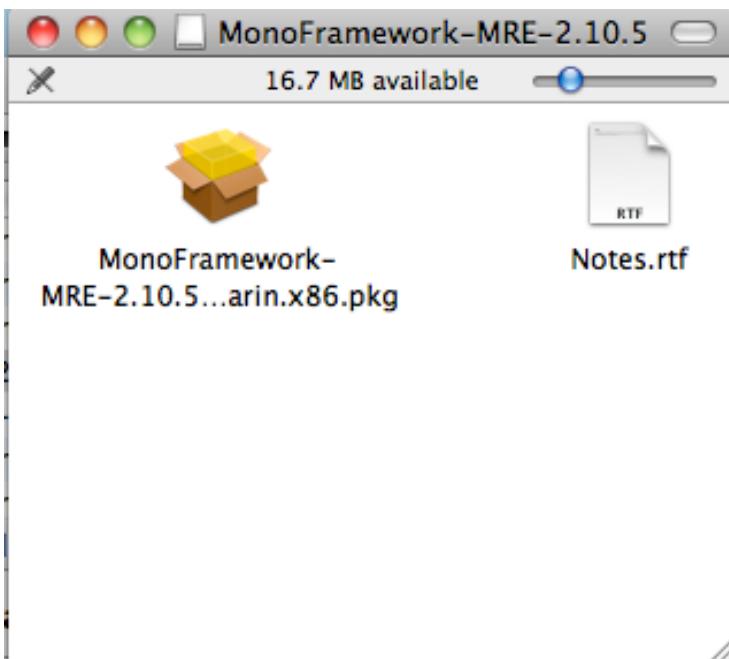


Figure 39.11: MonoFramework

El instalador se abre y ejecuta:

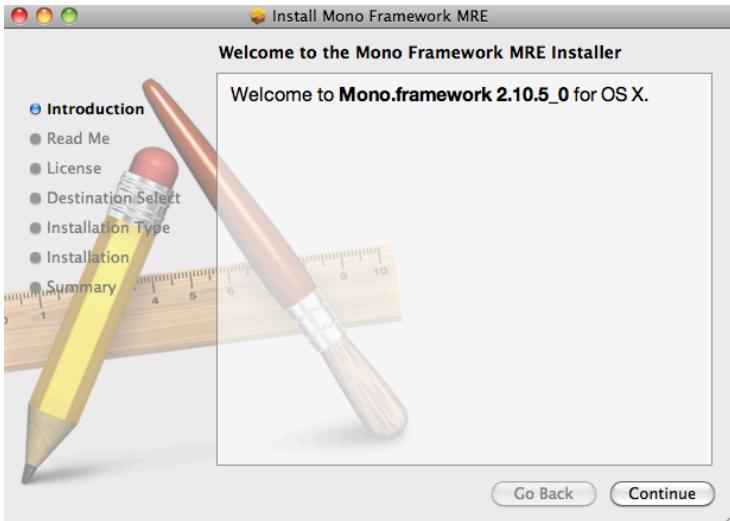


Figure 39.12: Instalando MonoFramework

Siga cada uno de los pasos, haga clic en “Continuar”, el siguiente paso es ver la sección ‘Read me’. Esta es información importante, ya que posee todos los archivos que el paquete instalará, incluyendo información sobre cómo desinstalar Mono:

Haga click en ‘Continue’ en la pantalla siguiente, la licencia. Aparecerá el cuadro de diálogo de acuerdo/desacuerdo. Si está de acuerdo con las condiciones de la licencia, la instalación continuará:

Los siguientes dos pasos de la instalación le pedirán que elija un destino y comprobar que haya espacio suficiente en el disco. Cuando la instalación se haya completado, verá la siguiente pantalla:

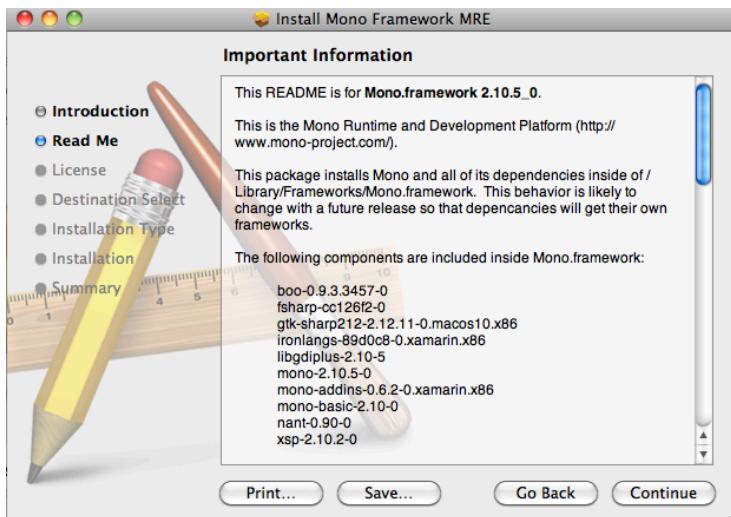


Figure 39.13: Readme de MonoFramework

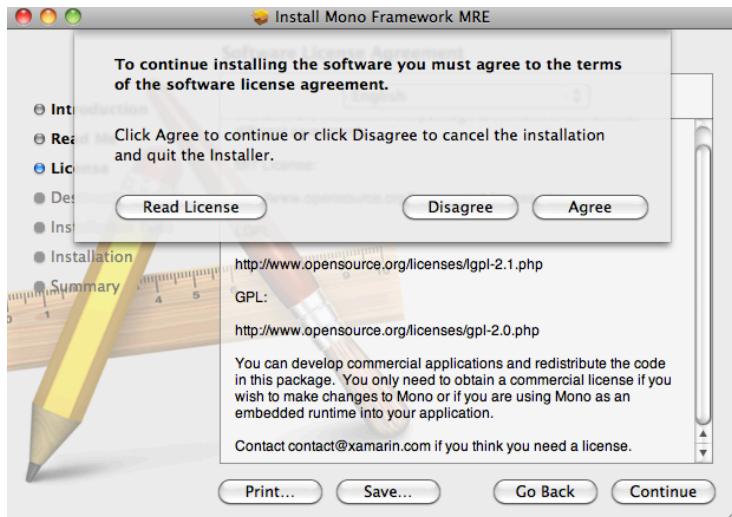


Figure 39.14: Acuerdo

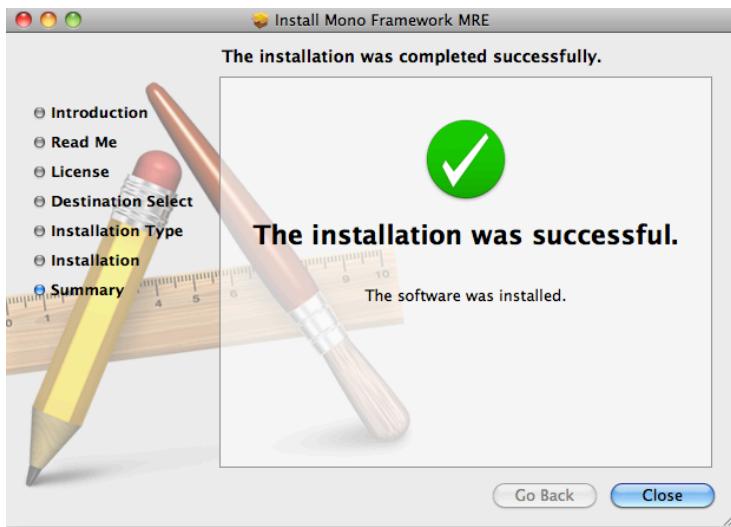


Figure 39.15: Instalación terminada

Ahora puede salir del instalador. A continuación, eche un vistazo a la imagen del disco KeePass, haga doble click para abrirlo y arrastre la aplicación KeePass a su carpeta de Aplicaciones:



Figure 39.16: Arrastrando a la carpeta de Aplicaciones

Ahora KeePass está listo para usar en Mac OS X.

# 40

## Cifrado de contraseñas con un administrador

Para cifrar contraseñas utilizamos KeePass en Windows, KeePassX en Ubuntu y KeyChain en OSX. El principio básico es el mismo: usted tiene un archivo en su computadora, que se cifra con una *contraseña única muy segura*. Esto se refiere a veces como una ‘contraseña maestra’, ‘contraseña de administrador’, ‘contraseña raíz’, etc, pero todos ellos son *la clave definitiva* para todas sus claves y otros datos seguros. Por esta razón no se puede ni se debe pensar a la luz sobre la creación de esta contraseña. Si un administrador de contraseñas es parte de su sistema operativo (como sucede con OSX) se desbloquea automáticamente para usted después de que usted ingrese a su cuenta y le permite acceder a información segura, como contraseñas. Por esto y otras razones, se debe desactivar ‘Iniciar sesión automáticamente’. Debería iniciar una sesión siempre que arranque el equipo y, mejor aún, debería configurarlo para que automáticamente la cierre o bloquee la pantalla después de un período de tiempo determinado

## Cifrado de contraseñas con KeePassX en Ubuntu

Abra primero KeePassX desde el menú Applications -> KeePassX.

La primera vez que utilice KeePassX es necesario establecer una nueva base de datos para almacenar sus contraseñas. Haga clic en File -> New Database.

Se le pedirá que establezca una clave principal (clave).

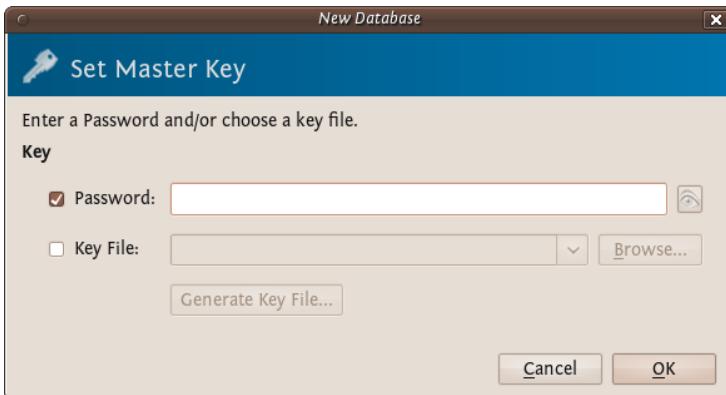


Figure 40.1: Estableciendo una clave principal

Elija una contraseña fuerte para este campo - consulte el capítulo acerca de contraseñas si desea algunos consejos sobre cómo hacer esto. Ingrese la contraseña y presione 'OK'. Se le pedirá que lo ingrese nuevamente. Hecho esto, presione 'OK'. Si las contraseñas son iguales verá una nueva 'base de datos' KeePassX lista para usar.

Ahora tiene un lugar para almacenar todas sus contraseñas y

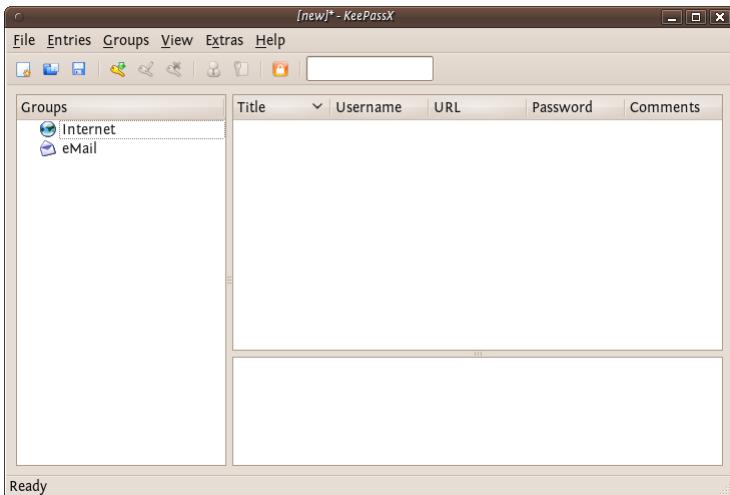


Figure 40.2: Ingresando la contraseña

protegerlas con la contraseña ‘maestra’ que acaba de establecer. Verá dos categorías por defecto ‘Internet’ y ‘Correo electrónico’ - se pueden almacenar las contraseñas sólo en estas dos categorías, puede eliminar categorías, añadir subgrupos, o crear nuevas categorías. Por ahora sólo nos quedaremos con estas dos y añadiremos la contraseña de nuestro correo electrónico al grupo de correo electrónico. Haga clic en esta categoría y seleccione “Agregar nueva entrada ...”:

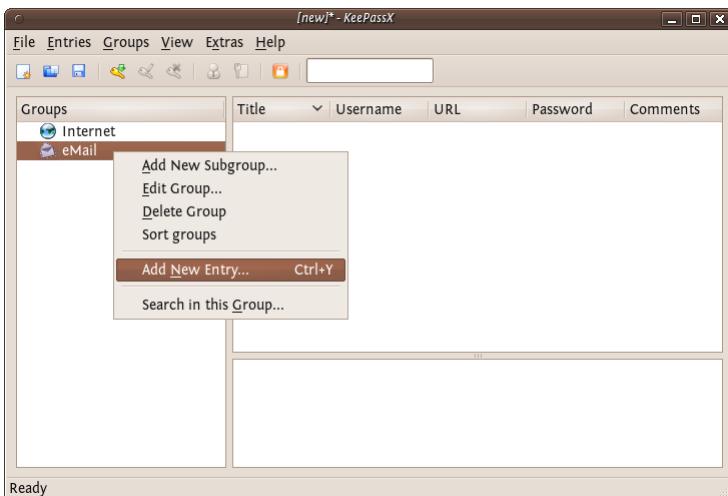


Figure 40.3: Agregando una nueva entrada

Así que ahora llene este formulario con los detalles para que usted pueda identificar correctamente la cuenta de correo electrónico y las contraseñas asociadas. Usted necesita llenar los campos ‘Título’ y los campos de la contraseña. Todo lo demás es opcional.

KeePassX da alguna indicación de si las contraseñas que se utilizan son ‘fuertes’ o ‘débiles’ ... usted debe tratar de hacer que las

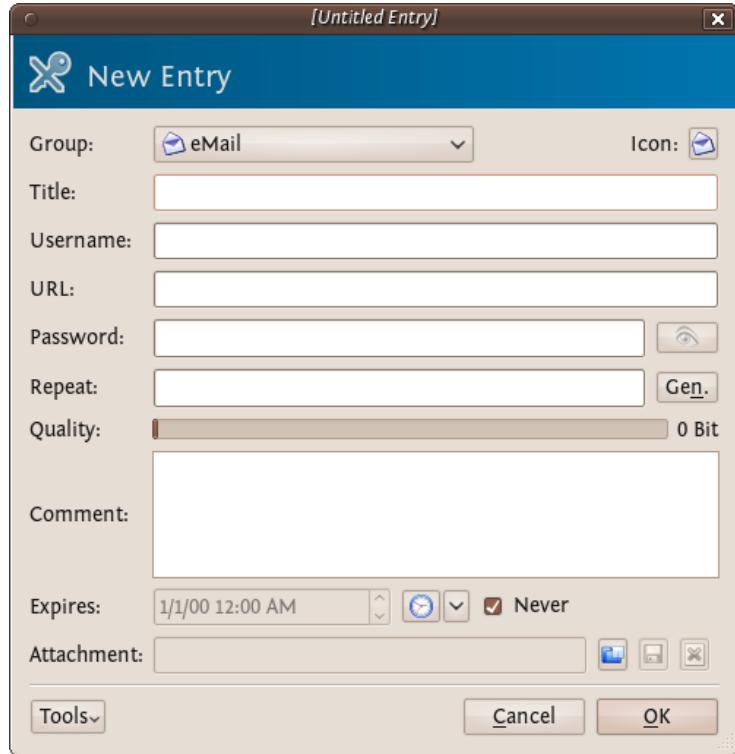


Figure 40.4: Nueva entrada

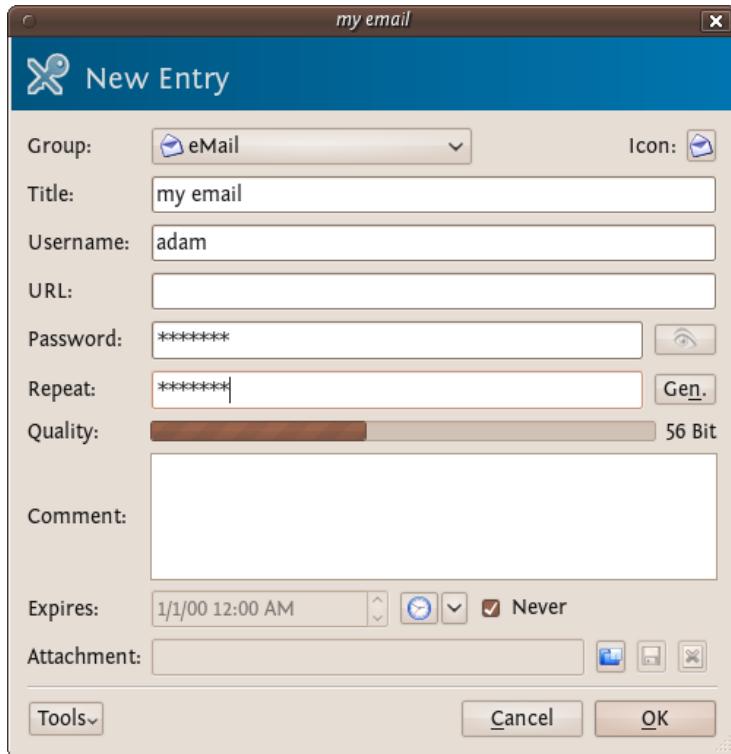


Figure 40.5: Formulario

---

contraseñas sean lo más fuertes posible; consejo sobre esto, lea el capítulo acerca de cómo crear una buena contraseña. Pulse ‘OK’ cuando haya terminado y usted verá algo como esto:

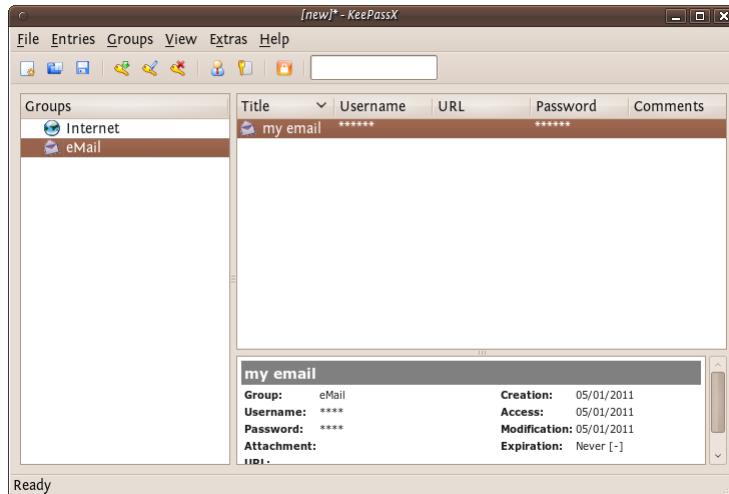


Figure 40.6: Contraseña en KeePassX

Para recuperar las contraseñas deberá hacer doble click en la entrada y verá la ventana que utilizó para registrar la información. Si hace click en el ícono del ‘ojo’ a la derecha de las contraseñas, pasarán de asteriscos (\*\*\*\*) a texto plano para que pueda leerlo.

Ahora usted puede utilizar KeePassX para almacenar sus contraseñas. Sin embargo, antes de emocionarse demasiado usted debe hacer una última cosa. Al cerrar KeePassX (elija File->Quit) se le pregunta si desea guardar los cambios que haya realizado.

Pulse “Sí”. Si es la primera vez que se utiliza KeePassX (o acaba de crear una nueva base de datos), debe elegir un lugar para almacenar sus contraseñas. De lo contrario, se guardará

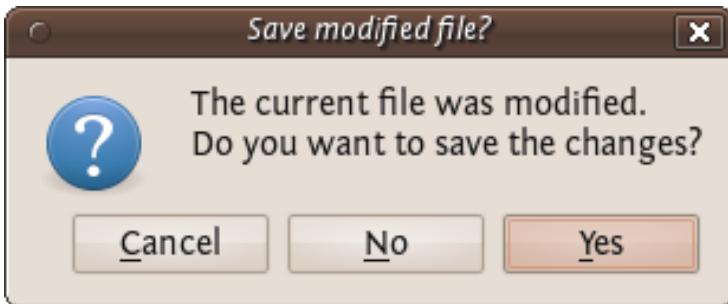


Figure 40.7: Grabando los cambios

la información actualizada en el archivo que ha creado anteriormente.

Si desea acceder a las contraseñas a continuación, debe abrir KeePassX y se le pedirá la clave maestra. Después de escribir esto usted puede agregar todas tus contraseñas de la base de datos y ver todas las entradas. No es una buena idea abrir KeePassX y tenerlo abierto permanentemente ya que alguien podría ver sus contraseñas si pueden acceder a su computadora. En lugar de entrar, en la práctica limítese a abrirlo cuando lo necesite y luego ciérrelo de nuevo.

## Cifrado de contraseñas con KeePass en Windows

Después de instalar KeePass en Windows se puede encontrar en el menú de aplicaciones. Inicie la aplicación y la siguiente ventana debe aparecer.

Se empieza haciendo una base de datos, el archivo que contendrá su clave. En el menú seleccione **File > new**. Usted tiene que

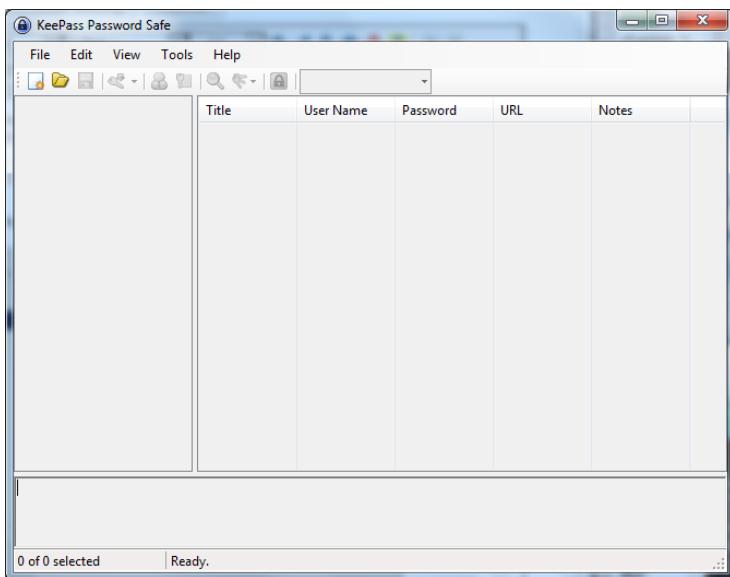


Figure 40.8: Lanzando KeePass

elegir el nombre y la ubicación del archivo en la ventana de diálogo siguiente. En este ejemplo llamamos a nuestra base de datos `my_password_database`.

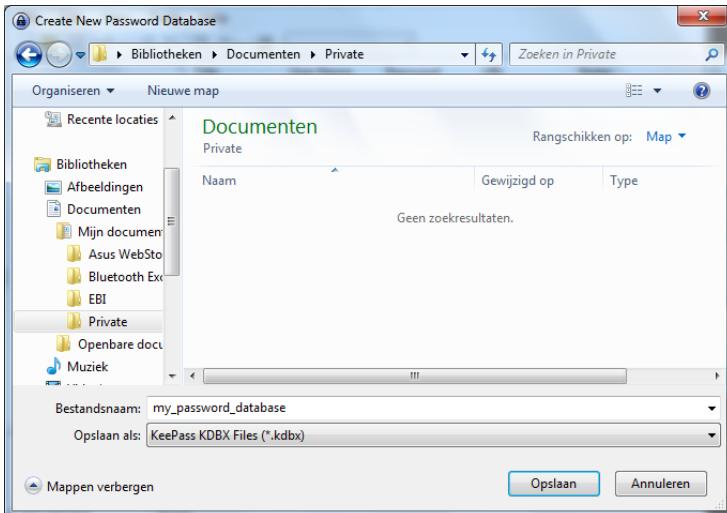


Figure 40.9: Nuestra base de datos

La siguiente pantalla le pedirá la contraseña maestra. Introdúzcala y haga click en 'OK'. Usted no tendrá que elegir otra cosa.

La siguiente ventana le permite añadir opciones especiales de configuración para su nueva base de datos. No es necesario modificar nada. Haga clic en 'Aceptar'.

Ahora aparece la ventana principal de nuevo y vemos algunas categorías de contraseñas por defecto en el lado izquierdo. Permite añadir una nueva contraseña en la categoría 'Internet'. Primero haga clic en la palabra 'Internet', luego pulse en el ícono de agregar entrada debajo de la barra de menús.

Aparecerá una ventana como la de abajo. Utilice los campos

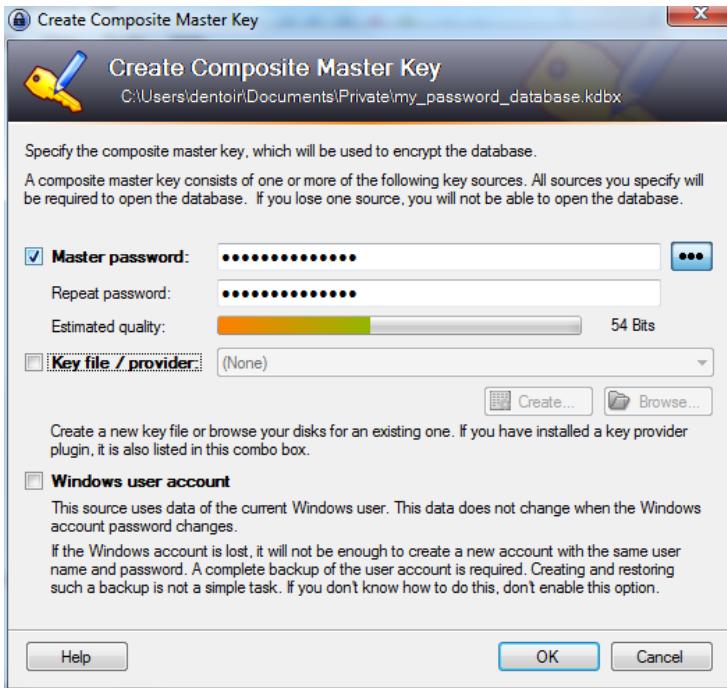


Figure 40.10: Contraseña maestra

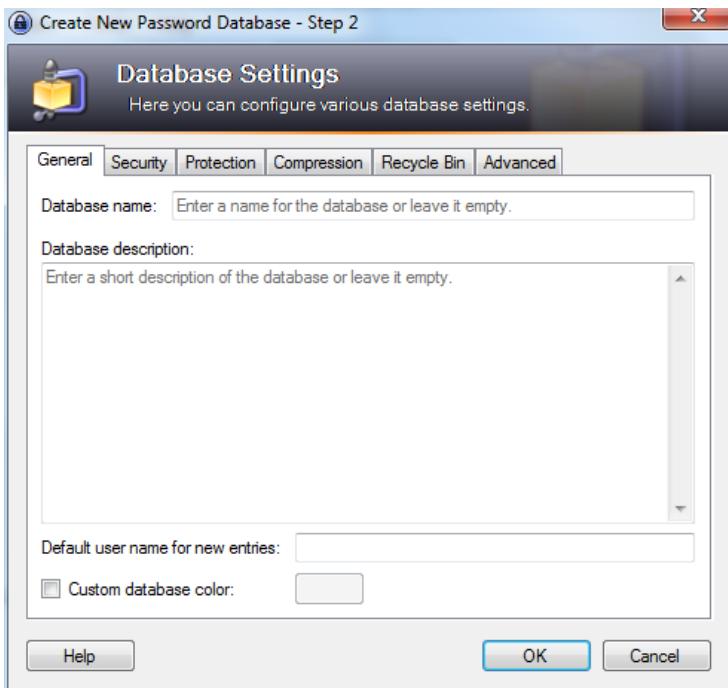


Figure 40.11: Opciones de configuración

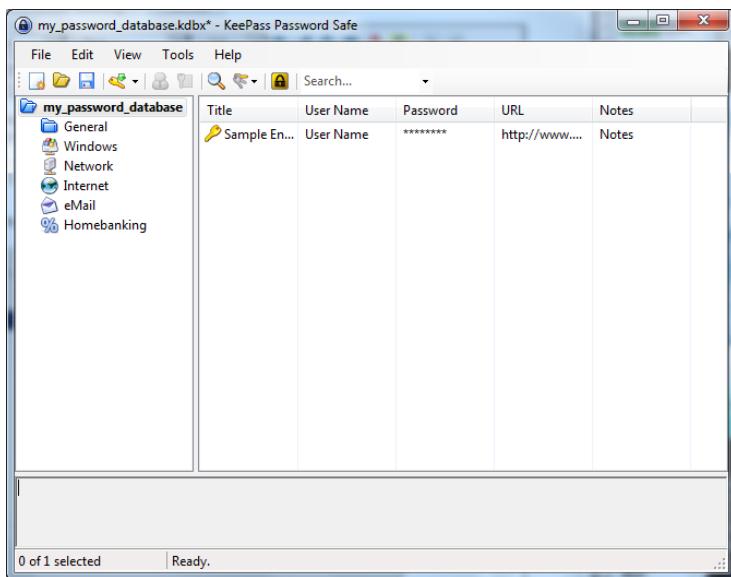


Figure 40.12: Categorías de Internet

para dar una descripción de esta contraseña especial, y por supuesto, ingresar la propia contraseña. Cuando termine, haga click en ‘OK’.

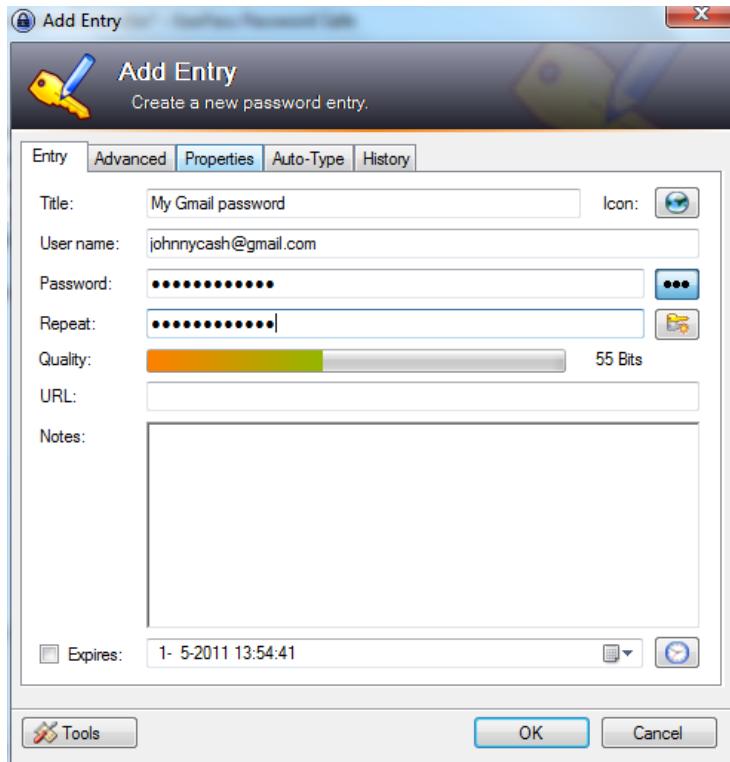


Figure 40.13: Descripción de contraseñas

---

## Contraseñas cifradas con Keychain en Mac OSX

Mac OSX viene preinstalado con el gestor de contraseñas ‘Keychain’. Debido a su estrecha integración con la mayoría de los OS la mayoría de las veces es casi imposible saber que existe. Pero de vez en cuando usted tendrá una ventana pop-up en casi cualquier aplicación preguntando ‘¿quiere guardar esta contraseña en Keychain?’. Esto sucede cuando se agregan nuevas cuentas de correo electrónico a su cliente de correo, cuando se accede a una red inalámbrica protegida, cuando introduce sus datos en el cliente de chat, etc, etc, etc.

Básicamente lo que ocurre es que Mac OS X le ofrece a usted almacenar todos los datos de usuario y contraseñas diferentes en un archivo cifrado que se abre tan pronto como se inicie sesión en su cuenta. A continuación, puede revisar su correo, iniciar sesión con su WiFi y utilizar el cliente de chat sin tener que introducir sus datos de acceso en todo momento una y otra vez. Este es un proceso totalmente automatizado, pero si usted quiere ver lo que está almacenado, dónde lo está, alterar contraseñas, o buscar una contraseña entonces tendrás que abrir el programa Keychain.

Usted puede encontrar el programa de llavero en la carpeta Utilities, que está dentro de la carpeta Applications.

Cuando lo abra, verá que su ‘Login’ de Keychain está desbloqueado y verá todos los elementos contenidos en el mismo en la parte inferior derecha de la ventana.

(Nota: la ventana aquí está vacía porque sería engañoso para el propósito de este manual hacer una captura de pantalla de mis claves personales y compartirlas con ustedes)

Puede hacer doble click en cualquiera de los elementos en Keychain para poder ver los detalles y marque la casilla ‘Show pass-

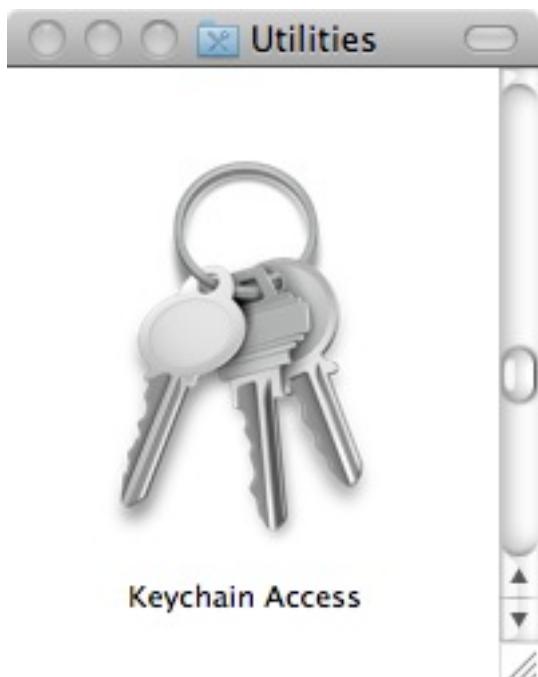


Figure 40.14: Contraseñas cifradas

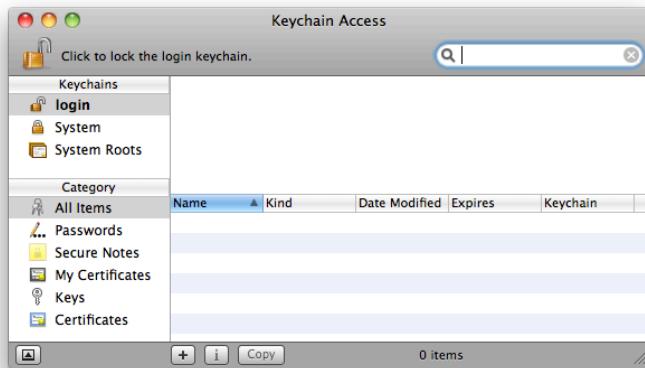


Figure 40.15: Claves personales

word:' para ver la contraseña asociada con el elemento.

Usted notará que se le pedirá su contraseña maestra o contraseña de inicio de sesión para ver el elemento.

Se puede acceder a modificar cualquiera de los elementos y también utilizar el Keychain para guardar con seguridad las partes y piezas de texto con las notas. Para ello haga click en las notas y elija 'New secure Note item' desde el menú archivo.



Figure 40.16: Mostrando las contraseñas



Figure 40.17: Contraseña maestra



# 41

## Obtención, configuración y prueba de una cuenta VPN

En todos los sistemas VPN, existe una computadora configurada como un servidor (en alguna país sin demasiadas restricciones), a la cual se conectan uno o más clientes. La configuración del servidor está fuera del alcance de este manual y la configuración de su sistema está cubierto, en general, por su proveedor de VPN. Este servidor es uno de los dos extremos del túnel cifrado. Es muy importante que la organización que provee el servidor sea confiable y esté ubicada en un país o región que también sea confiable. Para correr una VPN, se necesita una cuenta en dicho servidor.

Por favor recuerde que cada cuenta puede usarse, a menudo, en un sólo dispositivo a la vez. Si quiere usar una VPN con un teléfono móvil y una computadora personal simultáneamente, es muy posible que necesite dos cuentas.

## Una cuenta de un proveedor comercial de VPN

Hay múltiples proveedores de VPN ahí afuera. Algunos le ofrecerán probarlo gratis por un tiempo, otros comenzarán a cobrarle una tarifa fija por mes. Busque un proveedor de VPN que ofrezca cuentas con OpenVPN - una solución libre disponible para GNU/Linux, OS X y Windows, además de Android e iOS.

Cuando elija un proveedor VPN debe considerar los siguientes puntos:

- Cuando menos información le sea pedida para registrar una cuenta mejor. Un proveedor de VPN verdaderamente preocupado por su privacidad sólo le pedirá una dirección de correo electrónico (¡haga una temporal!), nombre de usuario y contraseña. No se necesita más, a menos que el proveedor cree una base de datos de usuarios, que es muy probable que no quieran ser parte de ello.
- Formas de pago que se utilizarán para pagar su suscripción: la transferencia de efectivo es probablemente el método más propenso a la privacidad, ya que no vincula su cuenta bancaria con su identificación en la red VPN. PayPal también puede ser una opción aceptable suponiendo que usted puede registrar y utilizar una cuenta temporal para cada pago. El pago a través de una transferencia bancaria o con tarjeta de crédito puede socavar gravemente su anonimato incluso más allá de la VPN.
- Evite los proveedores de VPN que le obliguen a instalar su propio software cliente propietario. Existen soluciones libres disponibles para todas las plataformas, y tener que ejecutar un cliente “especial” es una clara señal de un servicio falso.
- Evite el uso de VPN basada en PPTP, dicho protocolo

---

presenta vulnerabilidades de seguridad. De hecho, si dos proveedores son iguales en todo, elija el que *no le ofrezca* PPTP.

- Busque un proveedor de VPN que está utilizando OpenVPN - una solución VPN libre y multiplataforma.
- Puertas de salida en los países de su interés: poder elegir entre varios países le permite cambiar su contexto geopolítico y aparentar provenir de una parte diferente del mundo. ¡Tiene que ser consciente de los detalles de la legislación y las leyes de privacidad de ese país en particular!
- Considere la política de anonimato con respecto a su tráfico: un proveedor de VPN seguro debe tener una política de no divulgación. La información personal, como nombre de usuario y los tiempos de conexión, tampoco se deben registrar.
- Se deben admitir dentro de VPN a la gran mayoría de los protocolos de Internet.
- Compare el precio con la calidad del servicio y su fiabilidad.
- Investigue todos los problemas conocidos en cuanto al anonimato de los usuarios que el proveedor de VPN podría haber tenido en el pasado. Mire en línea, lea los foros y pregunte por ahí. No se deje tentar por nuevas ofertas o proveedores desconocidos, baratos o poco fiables.

Hay disponibles en varios sitios web comparaciones entre distintos servicios VPN que lo pueden ayudar a seleccionar la mejor opción:

- Best VPN Service
- VPN Creative
- Cship

## Configuración de su cliente VPN

“OpenVPN [...] es una solución completa de software VPN SSL que integra capacidades de servidor OpenVPN, capacidades de administración simplificada, interfaz de usuario OpenVPN Connect, y paquetes de software cliente de OpenVPN que se adaptan a GNU/Linux, OSX, Windows y entornos. El servidor OpenVPN Access es compatible con una amplia gama de configuraciones, incluyendo acceso remoto seguro y granular a la red interna y a los recursos privados en la red y a las aplicaciones en la nube con un control de acceso riguroso.” (<http://openvpn.net/index.php/access-server/overview.html>)

Hay muchos estándares diferentes para configurar VPN, incluyendo PPTP, LL2P/IPSec y **OpenVPN**. Varían en complejidad, nivel de seguridad provisto y disponibilidad de sistemas operativos. No use PPTP porque presenta importantes fallas de seguridad. En este manual nos concentraremos en OpenVPN. Funciona en la mayoría de versiones de GNU/Linux, OSX y Windows. OpenVPN se basa en TLS/SSL - usa el mismo tipo de **cifrado** que usa HTTPS (HTTP segura) y una gran cantidad de otros protocolos de cifrado. El cifrado de OpenVPN se basa en el algoritmo de intercambio de claves **RSA**. Para poder establecer una comunicación, tanto el servidor como el cliente necesitan claves RSA públicas y privadas.

Una vez que obtiene el acceso a una cuenta VPN el servidor genera las claves y usted simplemente necesita descargarlas del sitio web de su proveedor o recibirlas por medio de un correo electrónico. Junto con sus claves recibirá un certificado de raíz (\*.ca) y un archivo de configuración principal (\*.conf o \*.ovpn). En la mayoría de los casos solamente se necesitan los siguientes

---

archivos para configurar y correr un cliente OpenVPN:

- **client.conf** (o client.ovpn) - archivo de configuración que incluye todos los parámetros necesarios. NOTA: en algunos casos las claves y los certificados pueden estar embebidos dentro del archivo de configuración principal. En tal caso los archivos mencionados más abajo no son necesarios.
- **ca.crt** (excepto en el archivo de configuración) - certificado de autoridad raíz de su servidor VPN, usado para firmar y comprobar otras claves emitidas por el proveedor.
- **client.crt** (excepto en el archivo de configuración) - su certificado de cliente, le permite comunicarse con su servidor VPN.

En base a su configuración particular, su proveedor VPN puede requerirle nombre de usuario y contraseña para autenticar su conexión. A menudo, por conveniencia, el nombre de usuario y la contraseña pueden grabarse en un archivo separado o agregado al archivo de configuración principal. En otros casos, se usa autenticación basada en claves, que se almacenan en un archivo separado:

- **client.key** (excepto en el archivo de configuración) - clave de autenticación de cliente, usada para autenticar el servidor VPN y establecer un canal de datos cifrado.

En la mayoría de los casos, a menos que sea necesario, no necesitará cambiar nada en el archivo de configuración, y (¡téngalo por seguro!) **¡nunca necesitará editar los archivos de certificación o las claves!** Todos los proveedores VPN tienen instrucciones detalladas acerca de la instalación. Lea y siga estas directrices para asegurarse de que su cliente VPN está configurado correctamente.

NOTA: Por lo general, sólo está permitido el uso de una clave

por conexión, por lo que probablemente no debería estar usando las mismas en dispositivos diferentes al mismo tiempo. Obtenga un nuevo conjunto de claves para cada dispositivo que va a utilizar con una VPN, o intente establecer un gateway VPN local (de un nivel más avanzado, no cubierto aquí).

Descargue sus archivos de configuración y de claves de OpenVPN y cópielos en un lugar seguro. Luego pase al capítulo siguiente.

## Configuración del cliente OpenVPN

En los capítulos siguientes se dan algunos ejemplos de configuración de software cliente OpenVPN. En cualquier distribución de GNU/Linux utilice su gestor de paquetes preferido e instale **openvpn \*\*** u **openvpn-client**.

Si desea utilizar OpenVPN en Windows u OSX, consulte:

- OpenVPN (interfaz Windows)
- Tunnel Blick (interfaz OSX)

## Advertencias...¡Cuidado!

Aunque un VPN ocultará su dirección IP, debido a la naturaleza de la mayoría de los VPN los metadatos de su pila TCP/IP y otra información de identificación puede ser enviada.

Esto puede parecer trivial, pero fíjese, un encabezado IP estándar tiene 20 bytes de tamaño, algunos de los cuales se llenan con información obvia (4 bytes para la IP origen, 4 bytes para la IP destino, etc.) pero algunos bytes del encabezado pueden tener otras opciones arbitrarias; el encabezado TCP tiene al menos 20 bytes también, con el potencial para otros 20. La

---

configuración específica de estas opciones varía según el sistema operativo, incluso según su versión, así como un simple paquete SYN de TCP es a menudo suficiente para identificar el sistema operativo en uso, la versión y otra información reveladora, como el tiempo de actividad del sistema. Existen herramientas fácilmente disponibles <http://lcamtuf.coredump.cx/p0f3/> que puede ser usado para obtener la huella de esta información; como prueba, intente conectarse a un servidor que ejecute esta herramienta con su conexión normal a Internet, luego conéctese nuevamente a través de su VPN. Muy probablemente verá que las huellas son idénticas, y que si su amigo se conecta su huella será diferente.

Por eso, es importante que recuerde lo siguiente: \* nadie irá a la cárcel por usted, si su proveedor VPN es alcanzado por una requisitoria legal para obtener información acerca de usted, ellos la brindarán. Porque declaren que no mantienen registros de actividad no significa que no los tengan. \* las VPN proveen privacidad, no anonimato



# 42

## VPN en Ubuntu

Si usa Ubuntu, puede conectarse a una VPN usando el *NetworkManager* incorporado. Esta aplicación es capaz de configurar redes con OpenVPN. No se debe usar PPTP por razones de seguridad. Desafortunadamente al momento de escribir este texto, no hay disponible en Ubuntu una interfaz L2TP. (Puede hacerse manualmente, pero está más allá del alcance de este documento).

El siguiente ejemplo explicara como conectarse con un servidor OpenVPN. En todos los casos supondremos que tiene una cuenta VPN.

### Preparación del Network Manager para redes VPN

Existe una excelente utilidad de red para Ubuntu: Network Manager. Es la misma utilidad que usted usa para configurar su red inalámbrica (o cableada)que está ubicada habitualmente en la esquina superior derecha de su pantalla (al lado del reloj).

Esta herramienta también es capaz de administrar VPN, pero antes de hacer esto, es necesario instalar algunas extensiones.

## Instalación de la extensión OpenVPN para Network Manager

Para instalar los plugins para Network Manager usaremos el Ubuntu Software Center.

1. Abra el Ubuntu Software Center escribiendo “software” en la barra de búsqueda Unity



Figure 42.1: Abriendo el Ubuntu Software Center

2. El Ubuntu Software Center habilita la búsqueda, instala y remueve software de su computadora. Haga click en la casilla de búsqueda en la esquina superior derecha de la ventana.
3. En la casilla de búsqueda, escriba “network-manager-openvpn-gnome” (es una extensión que habilitará OpenVPN). Es necesario tipar los nombres completos. Estos paquetes incluyen todos los archivos necesarios para establecer una conexión VPN exitosa.



Figure 42.2: Casilla de búsqueda

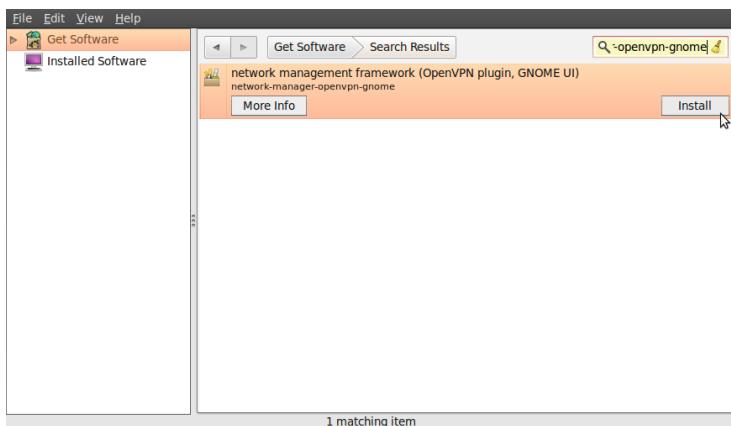


Figure 42.3: Buscando el software

4. Ubuntu puede pedirle permisos adicionales para instalar el programa. Si este es su caso, tipee su contraseña y haga click en Authenticate. Una vez instalados los paquetes, puede cerrar la ventana del Software Center.

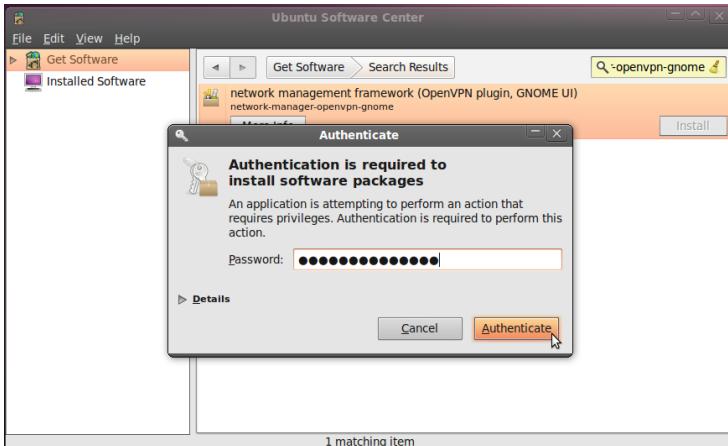


Figure 42.4: Instalando los paquetes necesarios

5. Para comprobar si las extensiones se instalaron correctamente, haga click en NetworkManager (el ícono a la izquierda de su reloj del sistema) y seleccione VPN Connections > Configure VPN.
6. Haga click en Add bajo la pestaña de VPN.
7. Si aparece un pop-up preguntando por el tipo de VPN y la opción de tecnología del túnel (OpenVPN) está disponible, esto significa que usted tiene instalada la extensión VPN correctamente. Si tiene lista la información de logueo a su VPN, puede continuar, en caso contrario debe adquirir una cuenta VPN de un proveedor. Si este es el caso, cancele y cierre el Network Manager.

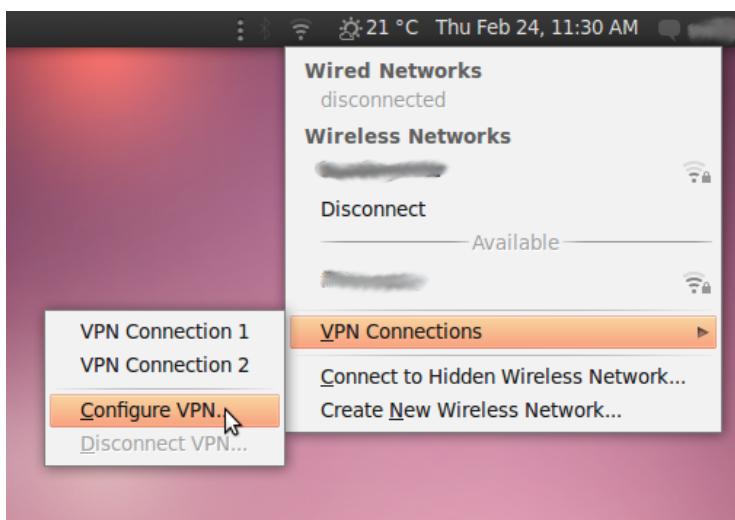


Figure 42.5: Abriendo VPN

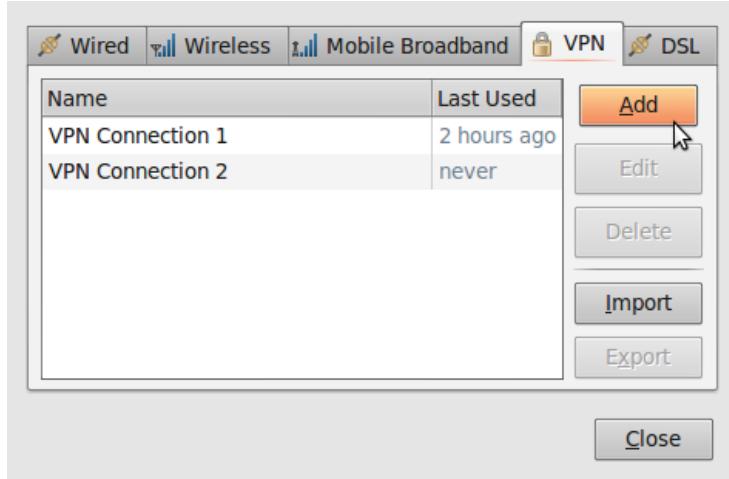


Figure 42.6: Agregando una conexión VPN



Figure 42.7: Creación de una cuenta VPN

---

## Configuración de una red OpenVPN

Supondremos que su proveedor de VPN ya le ha entregado a usted sus archivos de configuración. Esta información debería consistir en lo siguiente:

- un archivo \*.ovpn, ex. air.ovpn
- El archivo ca.crt (específico de cada proveedor OpenVPN)
- El archivo user.crt (este archivo es su certificado personal, usado para cifrado de datos)
- El archivo: user.key (este archivo contiene su clave privada. Debería ser protegido cuidadosamente. Perder este archivo volverá insegura a su conexión)

En la mayoría de los casos su proveedor le enviará estos archivos a usted en un archivo comprimido. Algunos proveedores de openvpn utilizan nombres de usuario y contraseña de autenticación que no están cubiertos.

1. Descomprima el archivo que ha descargado en una carpeta de su disco rígido rígido (por ejemplo: “/home/[sunombredeusuario]/.vpn”). Debería tener ahora cuatro archivos. El archivo “air.ovpn” es el archivo de configuración que usted necesita importar en NetworkManager.
2. Para importar el archivo de configuración, abra NetworkManager y vaya a VPN Connections > Configure VPN.
3. Bajo la pestaña VPN, pulse Import.
4. Localice el archivo air.ovpn que ha descomprimido. Pulse Open.
5. Se abrirá una nueva ventana. Deje todo como está y seleccione Apply.
6. ¡Felicitaciones! Su conexión VPN está lista para ser usada y debería aparecer en la lista de conexiones bajo la pestaña

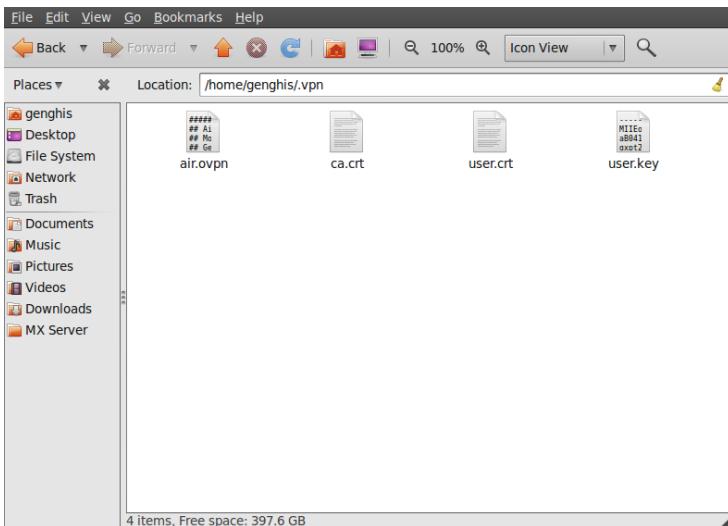


Figure 42.8: Archivo de configuración



Figure 42.9: Configurando VPN



Figure 42.10: Importando el archivo

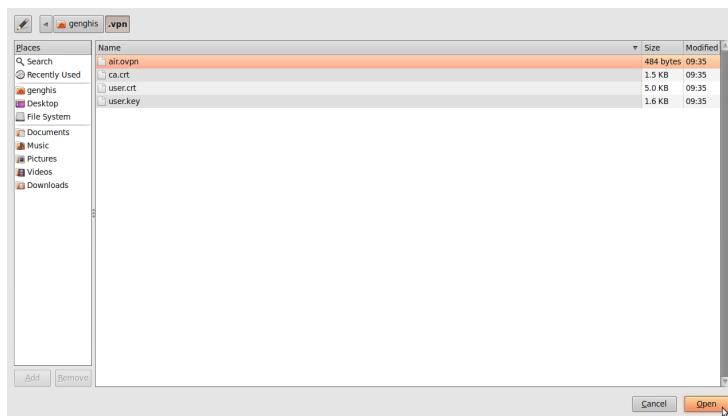


Figure 42.11: Abriendo air.ovpn

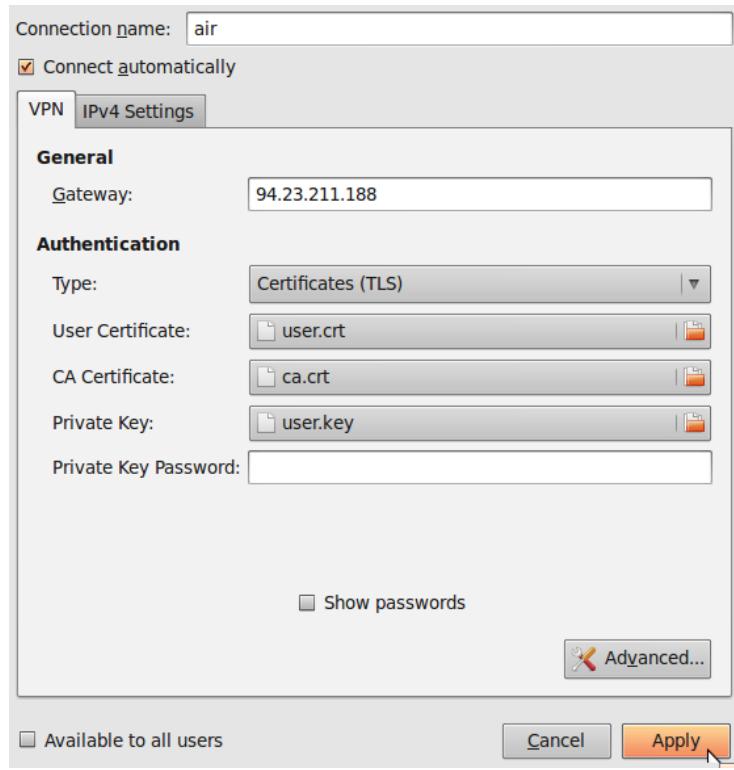


Figure 42.12: Terminando la configuración

VPN. Ahora puede cerrar NetworkManager.



Figure 42.13: Cerrando Network Manager

## Uso de su nueva conexión VPN

Ahora que ha configurado NetworkManager para conectarse a un servicio VPN usando el cliente OpenVPN, puede usar su nueva conexión VPN para eludir la censura en Internet. Para comenzar siga estos pasos:

1. En el menú NetworkManager, seleccione su nueva conexión de VPN Connections.
2. Espere que se establezca la conexión VPN. Cuando está conectado, un pequeño candado aparecerá justo arriba del ícono de NetworkManager, indicando que usted ahora está

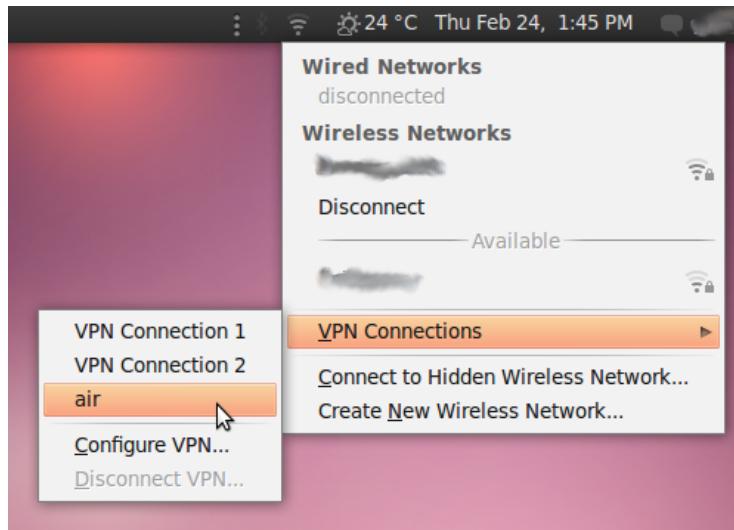


Figure 42.14: Buscando la conexión VPN

usando una conexión segura. Mueva el cursor sobre el ícono para confirmar que su conexión VPN está activa.

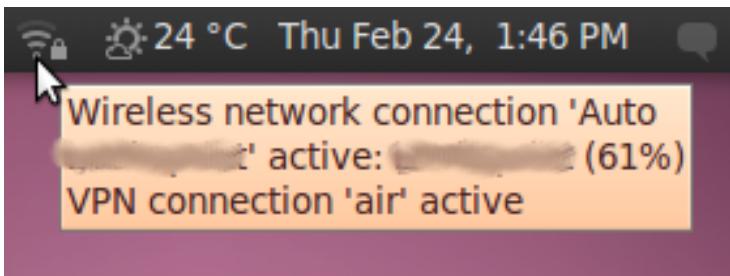


Figure 42.15: Conexión activa

3. Compruebe su conexión, usando el método descripto en la sección “Asegúrese que funciona” en este capítulo.
4. Para desconectarse de su VPN, seleccione VPN Connections > Disconnect VPN en el menú NetworkManager. Ahora está usando su conexión normal nuevamente.



Figure 42.16: Desconectando VPN



# 43

## VPN en MacOSX

Configurar un servicio VPN en MacOSX es muy sencillo una vez que tiene habilitada su cuenta. Supondremos que ya tiene en su poder las credenciales suministradas por su proveedor de VPN, para establecer una conexión L2TP/IPSec. Esta información debería contener lo siguiente:

- Nombre de usuario, por ejemplo `bill2`
- Contraseña, por ejemplo `verysecretpassword`
- servidor VPN, por ejemplo `tunnel.greenhost.nl`
- Una clave pre-compartida o un certificado de máquina

## Configuración

1. Antes de comenzar, por favor asegúrese de leer el párrafo “prueba antes y después de configurar una cuenta”, para comprobar si su conexión trabaja correctamente.
2. Un servicio VPN se configura en network settings, que son accesibles por medio de “System Preferences..” en el menú de Apple.

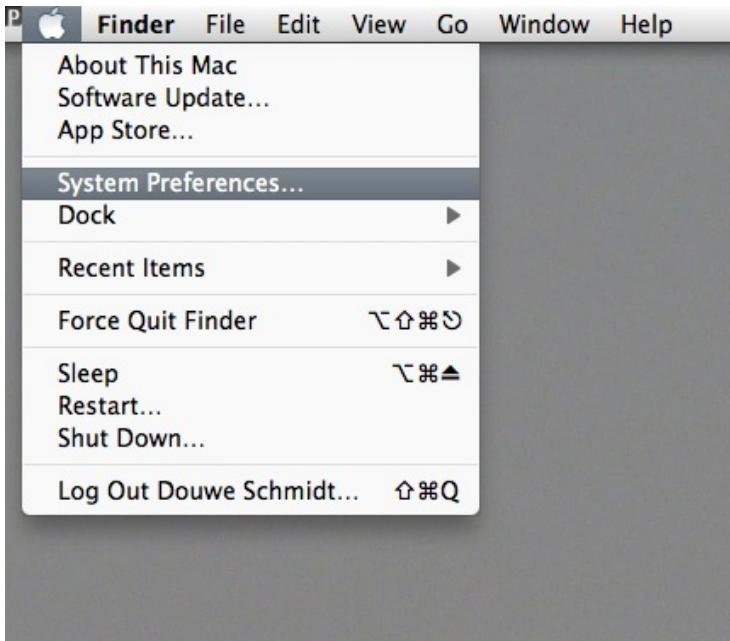


Figure 43.1: Configurando VPN

---

3. Abra Network preferences.

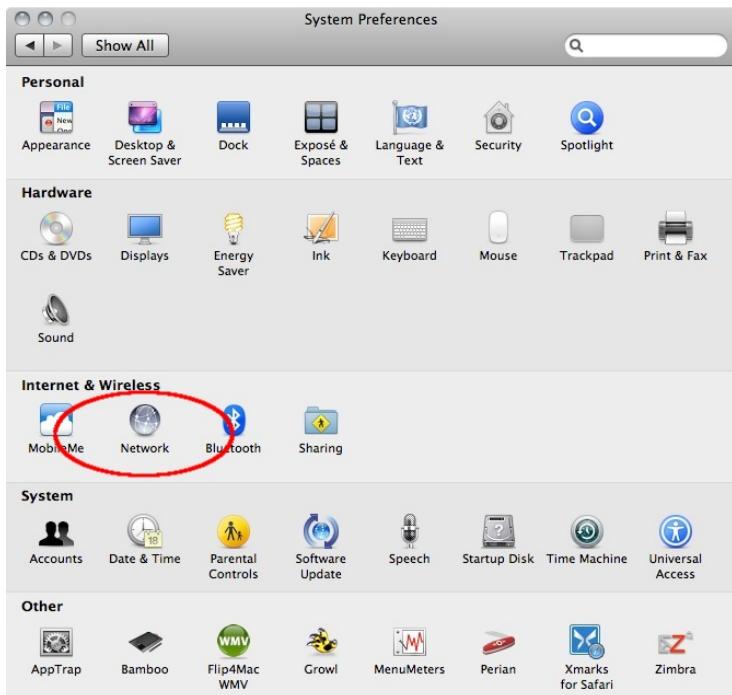


Figure 43.2: Preferencias de red

4. OSX usa este sistema para bloquear la pantalla. Para agregar una VPN es necesario desbloquearla, haciendo doble click en el candado de la parte inferior izquierda de su pantalla.
5. Ingrese sus credenciales.
6. Ahora puede agregar una nueva red, haciendo click en el signo “+”.

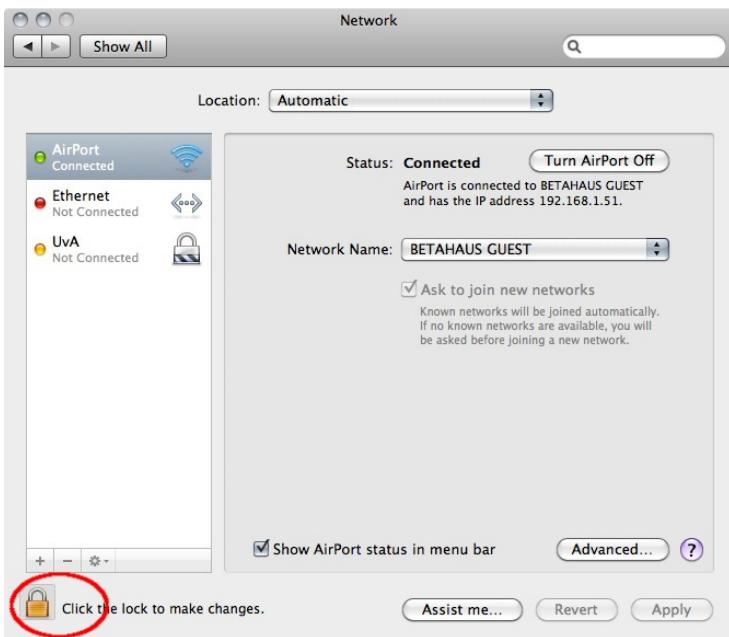


Figure 43.3: Desbloqueo de VPN

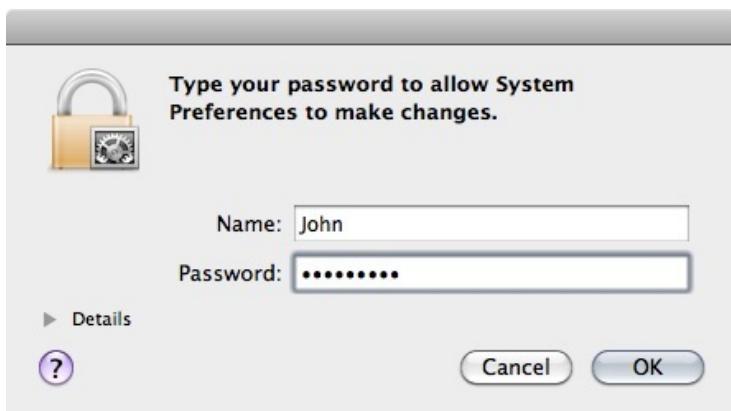


Figure 43.4: Ingresando credenciales

7. En la ventana emergente deberá especificar el tipo de conexión. En este caso elija una interfaz VPN con L2TP sobre IPSec. Es el sistema más común. No olvide darle a la conexión un nombre bonito.
8. Sigamos con los datos de conexión. Complete el nombre del servidor del proveedor y su nombre de usuario (denominado ‘Account Name’). Hecho esto, pulse el botón “Authentication Settings...”.
9. En la nueva ventana emergente puede especificar la información de la conexión. Esta es la manera en que el usuario y la máquina se autentifican. El usuario generalmente se autentifica con una contraseña, aunque se podrían usar otros métodos. La autenticación es realizada a menudo por un secreto compartido (Pre-Shared-Key/PSK), pero también muy a menudo mediante el uso de un certificado. En este caso se utiliza el método del secreto compartido. Hecho esto, haga click en OK.

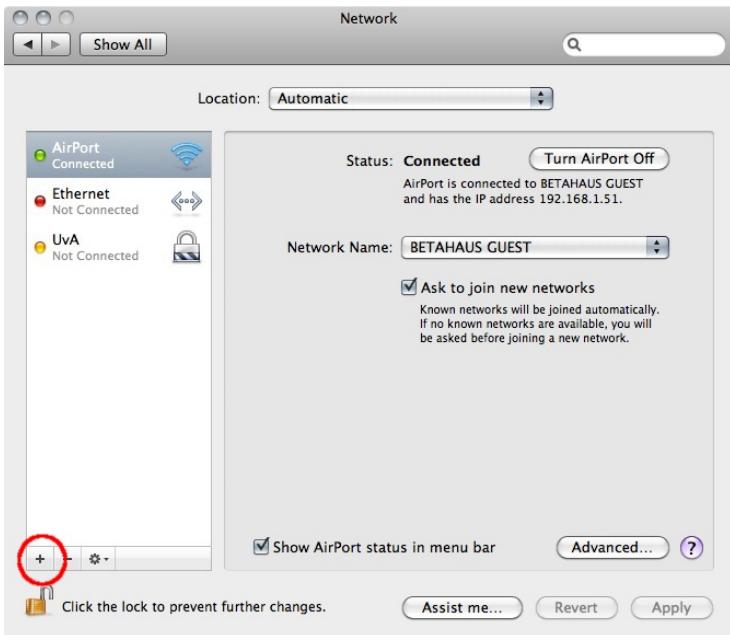


Figure 43.5: Agregando una nueva red

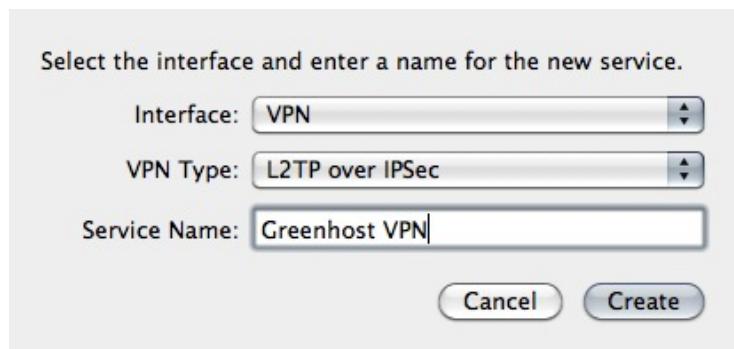


Figure 43.6: Estableciendo un nombre

10. Volvamos a la pantalla de red. El próximo paso es muy importante, por eso haga click en “Advanced...”
  11. En la nueva ventana emergente verá la opción para enrutar todo el tráfico a través de una conexión VPN. Habilítela para cifrar todo su tráfico.
  12. Bueno, hemos terminado. ¡Ahora conéctese!
  13. Aparecerá una ventana emergente. Para confirmar los cambios, sólo pulse “Apply”
  14. Después de unos pocos segundos, en el lado izquierdo la conexión debe tornarse verde. Si esto sucede, entonces ¡ya está conectado!
  15. Ok, ahora pruebe su conexión VPN en Windows
- 

Configurar un servicio VPN en MacOSX es muy sencillo una vez que tiene habilitada su cuenta. Supondremos que ya tiene en su poder las credenciales suministradas por su proveedor de VPN, para establecer una conexión L2TP/IPSec. Esta información debería contener lo siguiente:

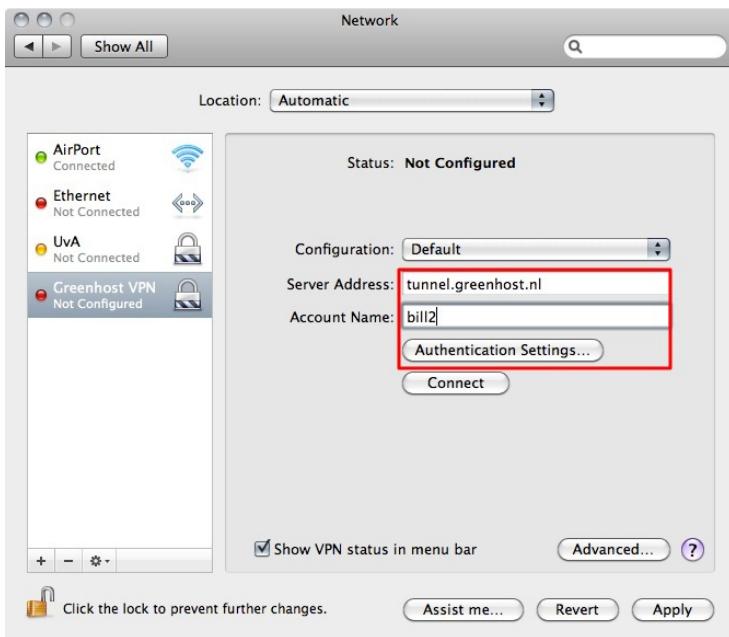


Figure 43.7: Configurando la autenticación



Figure 43.8: Configurando la autenticación

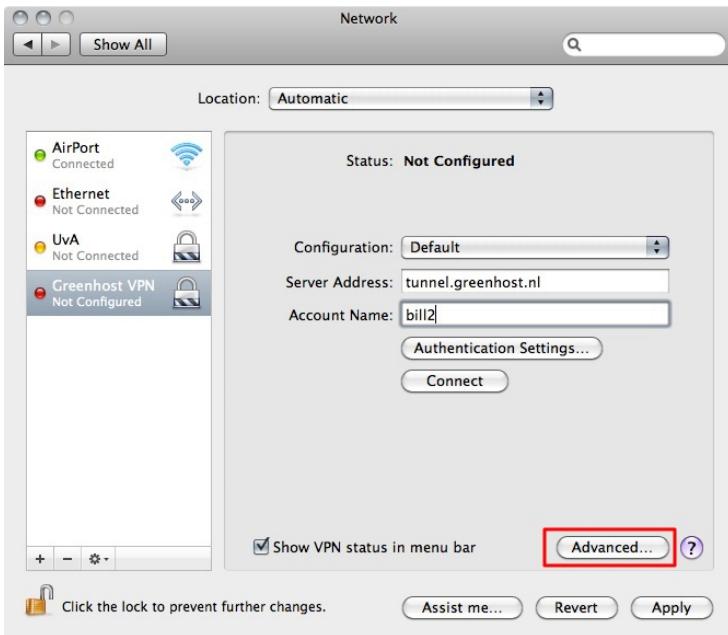


Figure 43.9: Pantalla de red

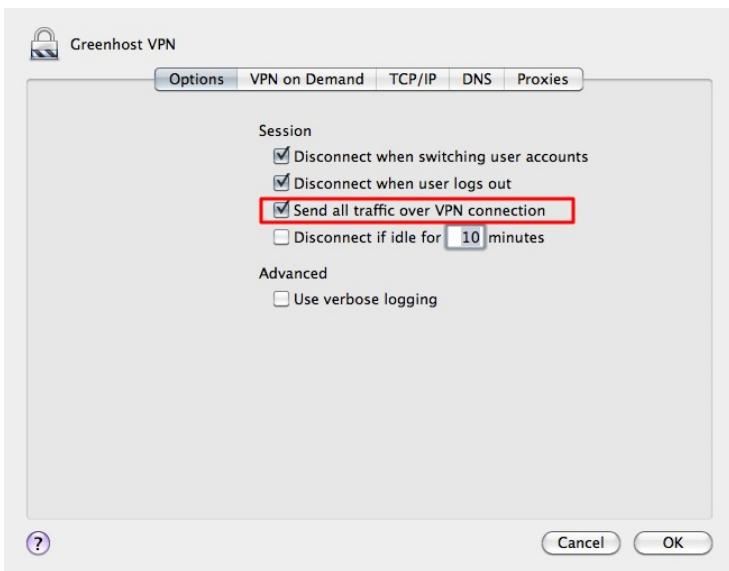


Figure 43.10: Cifrando el tráfico

## VPN en MacOSX

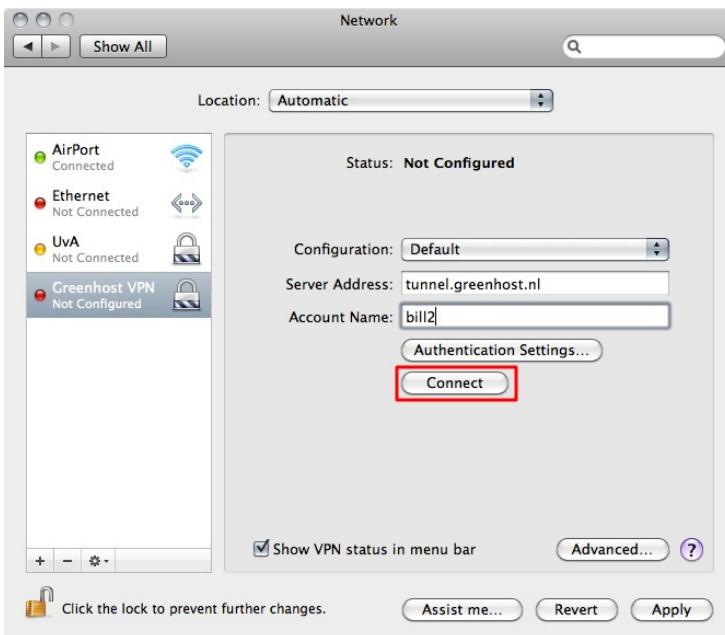


Figure 43.11: Conectándose...



Figure 43.12: Confirmando cambios

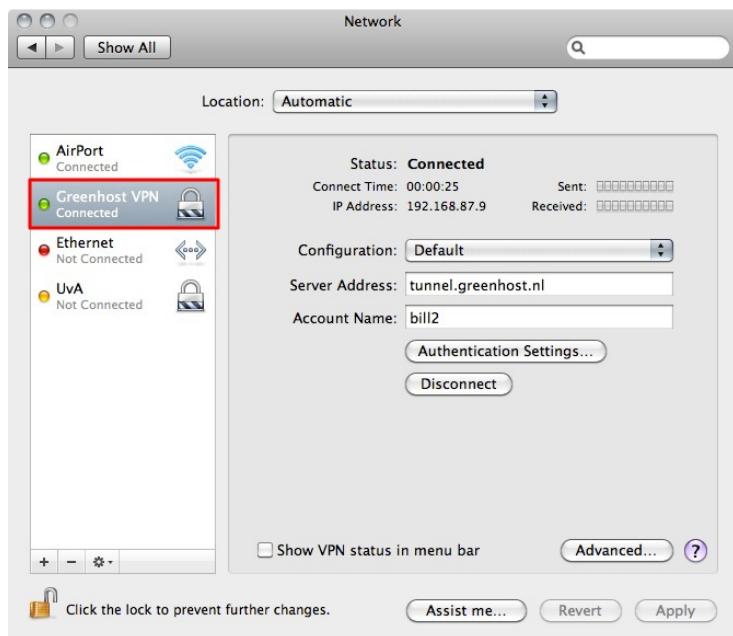


Figure 43.13: ¡Conexión establecida!

- Nombre de usuario, por ejemplo `bill2`
- Contraseña, por ejemplo `verysecretpassword`
- servidor VPN, por ejemplo `tunnel.greenhost.nl`
- Una clave pre-compartida o un certificado de máquina

## Setup

1. Antes de comenzar, por favor asegúrese de leer el párrafo “prueba antes y después de configurar una cuenta”, para comprobar si su conexión trabaja correctamente.
2. Necesitamos ir al “Network and Sharing Center” de Windows para crear una nueva conexión VPN. Nosotros podemos acceder fácilmente haciendo click en el ícono de red cercano al reloj de sistema.
3. Aparecerá el “Network and Sharing Center”. Revise la información referida a su red actual. Seleccione “Connect to a network” para añadir una conexión VPN.
4. El asistente de configuración aparecerá. Seleccione la opción “connect to a workplace”, que es el nombre dado por Microsoft a una conexión VPN.
5. La próxima pantalla le preguntará si desea usar su conexión a Internet o una antigua conexión por línea telefónica para conectarse a una VPN. Elija la primera opción.
6. La próxima pantalla le pedirá los detalles de su conexión. Ingrese aquí el servidor de su proveedor de VPN (denominado “Internet address” en este diálogo). En la parte inferior, por favor marque la casilla “No conectarse ahora; sólo configurar”. Con esta opción, la conexión se guarda automáticamente y es más fácil controlar la configuración extra. Hecho esto, pulse el botón “next”

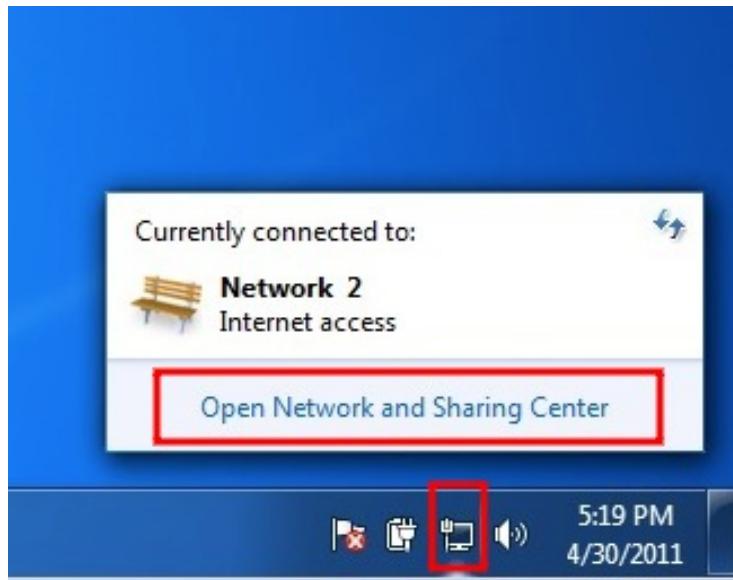


Figure 43.14: Creación de una cuenta VPN

## VPN en MacOSX

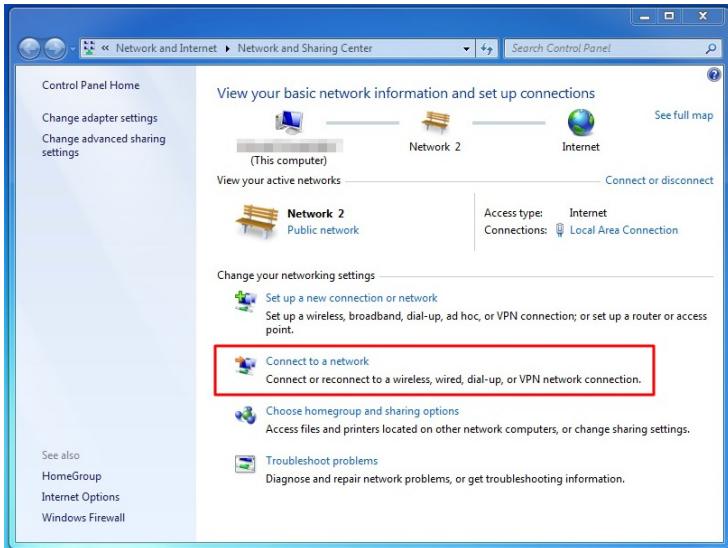


Figure 43.15: Añadiendo una cuenta VPN

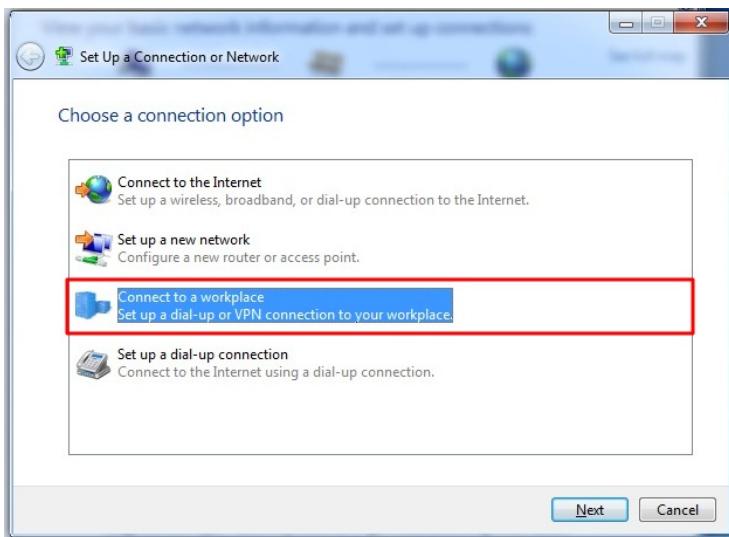


Figure 43.16: Asistente de configuración de VPN

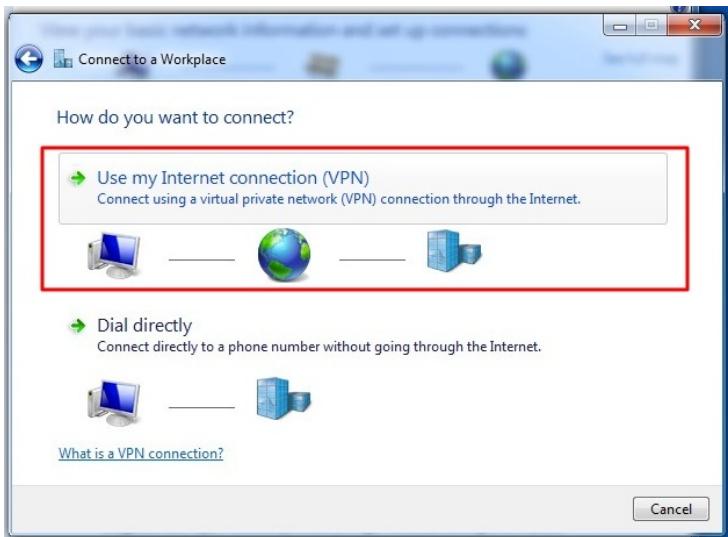


Figure 43.17: Seleccionando la conexión

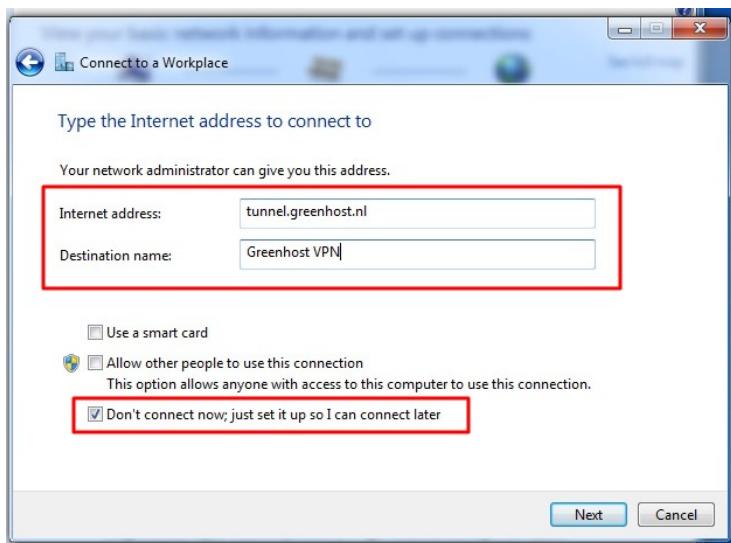


Figure 43.18: Detalles de conexión

7. Lo siguiente es su nombre de usuario y contraseña. Sólo tiene que ingresar los datos recibidos de su proveedor de VPN. Si falla la conexión, Windows los olvida. Así que recuérdelos, tal vez los necesite más tarde. Despues de esto, pulse “create”.



Figure 43.19: Datos del usuaario

8. Ya está disponible su conexión, si hace click en el ícono de red nuevamente, verá una nueva opción en el menú de red, el nombre de su conexión VPN. Conéctese haciendo click sobre ella.
9. Pulse “connect”
10. Aparecerá un diálogo de conexión VPN. Se le ofrece la oportunidad de revisar su configuración y conexión. Puede intentas conectarse, Windows tratará de descubrir el



Figure 43.20: Opciones de conexión



Figure 43.21 Conectándose

398

---

resto de la configuración automáticamente. Desafortunadamente, no siempre funciona, por eso, si no le es muy trabajoso, pulse el botón “properties”.

11. La ventana de propiedades aparecerá. La página más importante es “Security”, haga click en la pestaña de seguridad para abrirla.
12. En la pestaña de seguridad puede especificar el tipo de VPN, normalmente L2TP/IPSec. No use PPTP que posee varias vulnerabilidades de seguridad. Para L2TP/IPSec eche un vistazo a Advanced settings.
13. En la ventana de Advanced Settings, puede especificar si está usando una clave pre-compartida o un certificado. Esto depende de su proveedor de VPN. Si ha recibido una clave pre compartida, seleccione esta opción y complétela con este valor. Presione OK, y volverá a la pantalla anterior. Pulse OK nuevamente.
14. De regreso a la ventana de conexión intente conectarse ahora. Complete con su nombre de usuario y contraseña.
15. Aparecerá una ventana emergente de conexión
16. ¡Online! No se olvide de comprobar que su VPN esté trabajando correctamente.



Figure 43.22: Revisando la configuración

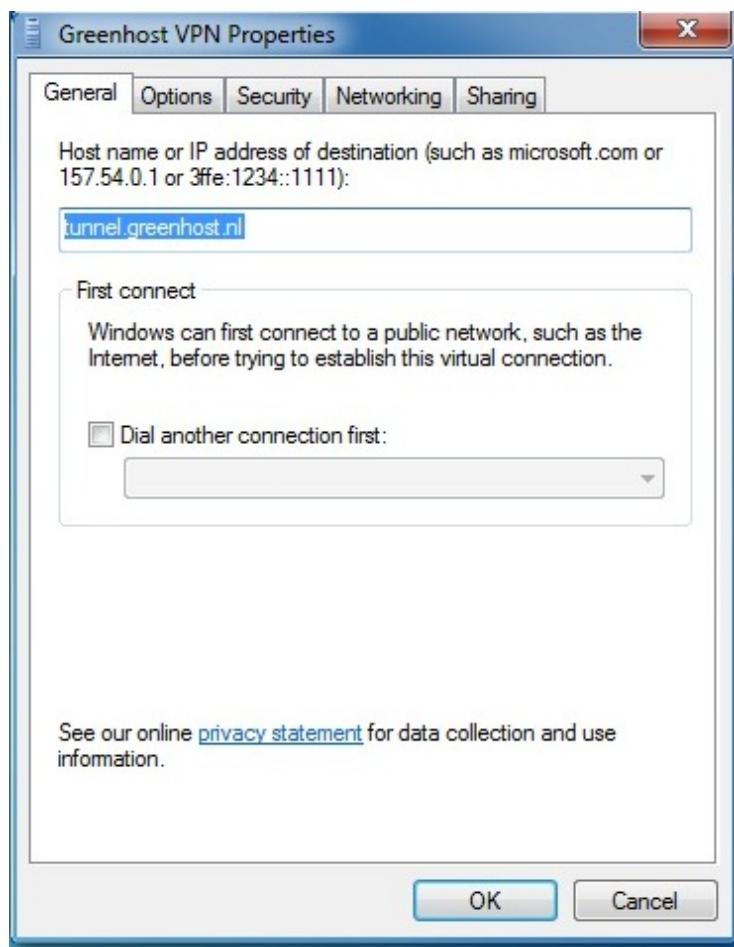


Figure 43.23: Seguridad

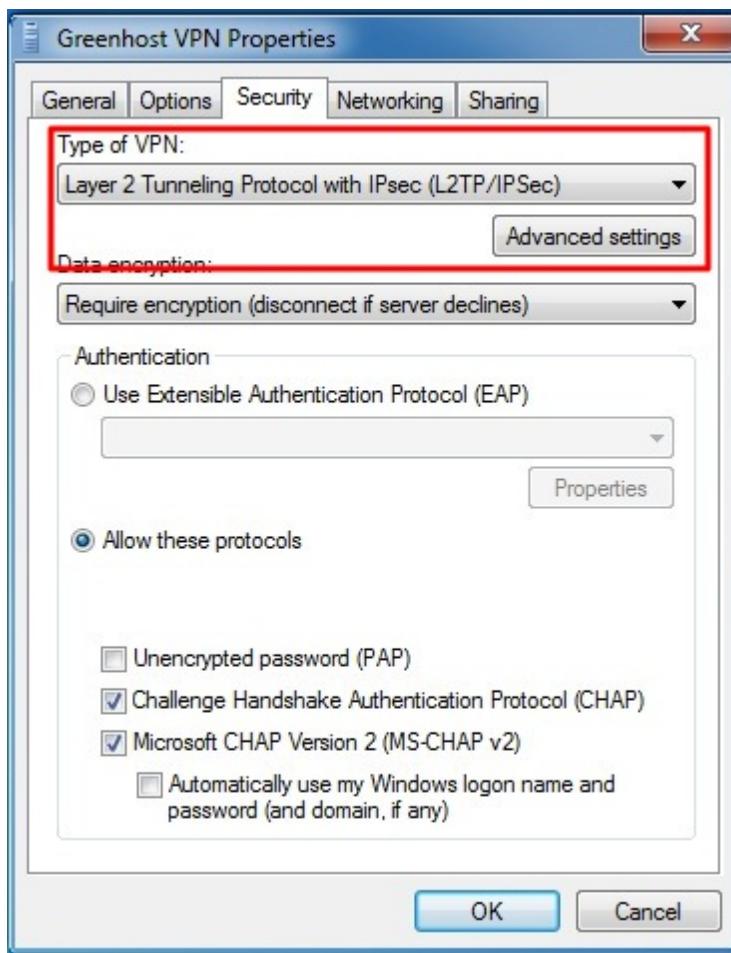


Figure 43.24: Tipo de VPN

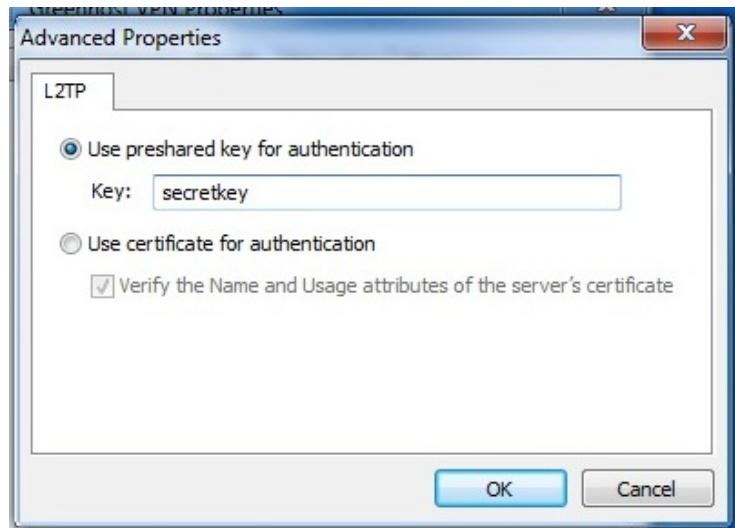


Figure 43.25: Configuración avanzada



Figure 43.26: Datos del usuario



Figure 43.27: Ventana de conexión



# 44

## Asegúrese que funcione

Probablemente una de las primeras cosas que debería asegurarse después que la conexión VPN se ha establecido correctamente es si sus datos realmente pasan a través de la red VPN. La prueba más simple (y fiable) es comprobar cuál es su dirección IP “externa” que está exponiendo en Internet.

Existen numerosos sitios web en línea que puede reportar su dirección IP y su ubicación geográfica (también llamada geolocalización). Muchos motores de búsqueda reportarán su dirección IP si busca “Mi IP”, pero también puede usar servidores dedicados como <http://www.myip.se> y <http://www.ipchicken.com>.

Verifique su dirección IP antes de conectarse a su VPN. Una vez conectado a su VPN, la dirección IP pública de su computadora debería cambiar por el brindado por su servidor VPN, y su geolocalización debería cambiar al lugar en donde su servidor VPN está localizado.

Una vez que sepa que su IP externa se ha cambiado a la IP de su servidor VPN, usted puede estar seguro de que su comunicación está cifrada.

Asegúrese que funcione

# 45

## Instalando TrueCrypt

TrueCrypt puede ser instalado en Windows, GNU/Linux, o Mac OSX. Los archivos de instalación están disponibles en su página web <http://www.truecrypt.org/downloads>

La sección siguiente explica detalladamente como instalar TrueCrypt en su computadora para diversos sistemas operativos, comenzando con Ubuntu.

### Instalación en Ubuntu

TrueCrypt no está disponible en los repositorios estándares de Ubuntu. Esto significa que no puede usar el centro de software Ubuntu o *apt-get* (el método de la línea de comandos para instalar software en Ubuntu). Además, debería visitar primeramente la página de descargas (<http://www.truecrypt.org/downloads>).

Usted verá primero un menú desplegable bajo el encabezado Linux.

Del menú desplegable ‘(Select a package)’ puede elegir una entre cuatro opciones:

*Linux*



Figure 45.1: Descarga de TrueCrypt

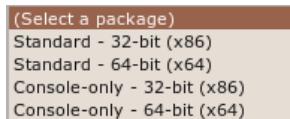


Figure 45.2: Seleccionando paquetes

Esta es una versión para instalar desde la consola - la que debe elegir si tiene habilidades técnicas y no quiere usar interfaces gráficas de usuario o si desea correr TrueCrypt en una máquina que sólo posea una terminal (línea de comandos o ‘shell’) de acceso (como un servidor remoto por ejemplo).

Suponiendo que usted ejecutará TrueCrypt en su computadora personal la mejor opción es la ‘standard’, la más sencilla, que le proporcionará una agradable interfaz de usuario. Debe elegir entre las dos opciones disponibles la más adecuada para la *arquitectura* de su máquina. ¿No sabe qué significa? Bueno, esto se relaciona básicamente con el tipo de hardware del procesador que posee su computadora, las opciones son 32-bits o 64-bits. Desafortunadamente Ubuntu no facilita información si no dispone de algunos conocimientos. Necesita abrir una desde el menú Aplicaciones->Accesorios y tipar

```
uname -a
```

La salida será algo como Linux bigsy 2.6.32-30-generic #59-Ubuntu SMP Tue Mar 1 21:30:46 UTC 2011 x86\_64

---

GNU/Linux. En esta instancia usted puede ver que la arquitectura es de 64-bit (`x86_64`). En este ejemplo debería elegir la opción ‘Standard - 64-bit (x64)’. Si lee `i686` en algún en la salida del comando `uname` entonces debería elegir la opción restante para descargar.

Una vez elegida presione el botón ‘download’ y grabe el archivo en su computadora.

El proceso de instalación aún no ha terminado. El archivo que ha descargado está comprimido (para acelerar la descarga) y debe descomprimirlo antes de instalarlo. Afortunadamente Ubuntu lo hace muy fácilmente - simplemente vaya al archivo en su computadora y haga click con el botón derecho sobre él y elija ‘Extraer aquí’.

Verá que aparece un nuevo archivo cerca del original comprimido:

¡Casi hemos terminado! Ahora haga click derecho sobre el nuevo archivo y elija ‘open’:

Si todo va bien verá una ventana abierta como esta:

Elija ‘Run’ y verá lo siguiente:

Ahora estamos llegando a alguna parte ... oprima el botón ‘Instalar TrueCrypt’. Se le mostrará un acuerdo de usuario. En la parte inferior elija “I accept and agree to be bound by the license terms” (suena serio). A continuación, se muestra otra pantalla de información que le dice que usted puede instalar TrueCrypt. Pulse ‘OK’ y luego se le pedirá la contraseña para instalar software en su ordenador. Introdúzcala y entonces por fin verá una pantalla como ésta:

Créalo o no ya está hecho...TrueCrypt está instalado y usted puede acceder desde el menú Aplicaciones->accesorios...cierra la ventana de configuración. Ahora vaya al capítulo Uso de TrueCrypt.

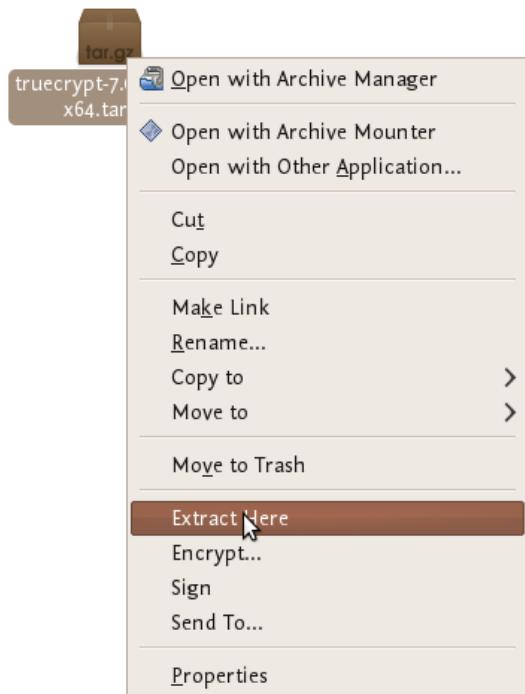


Figure 45.3: Extracción del archivo

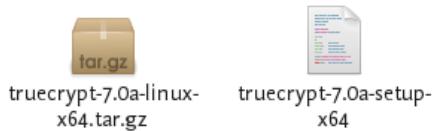


Figure 45.4: Archivo extraído

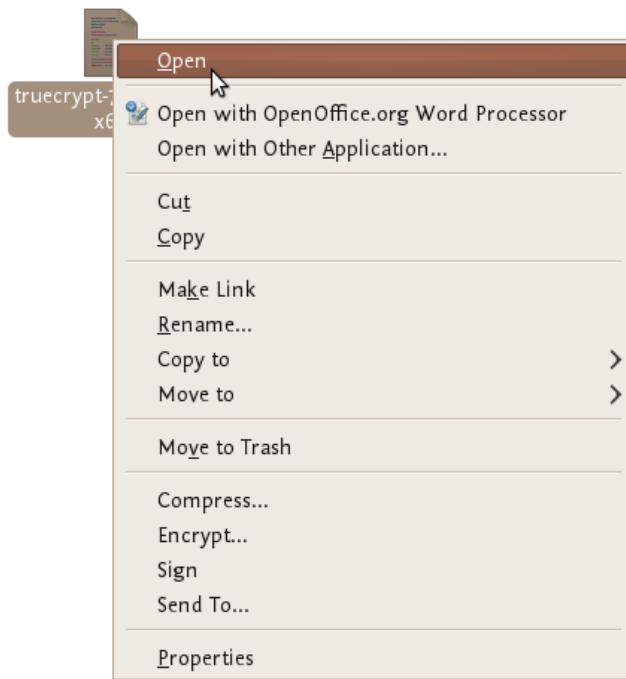


Figure 45.5: Abriendo el archivo



Figure 45.6: Ventana de instalación

## Instalando TrueCrypt

---

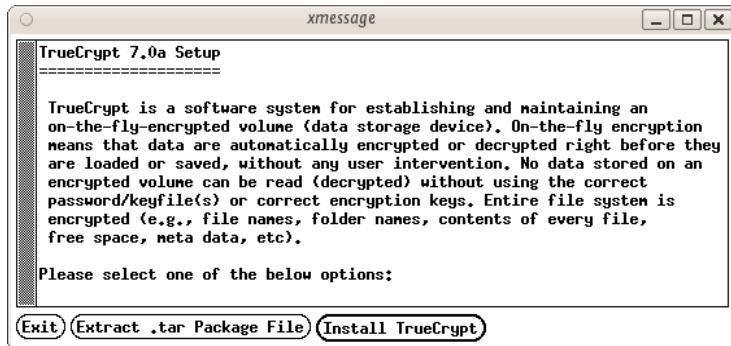


Figure 45.7: Instalando TrueCrypt

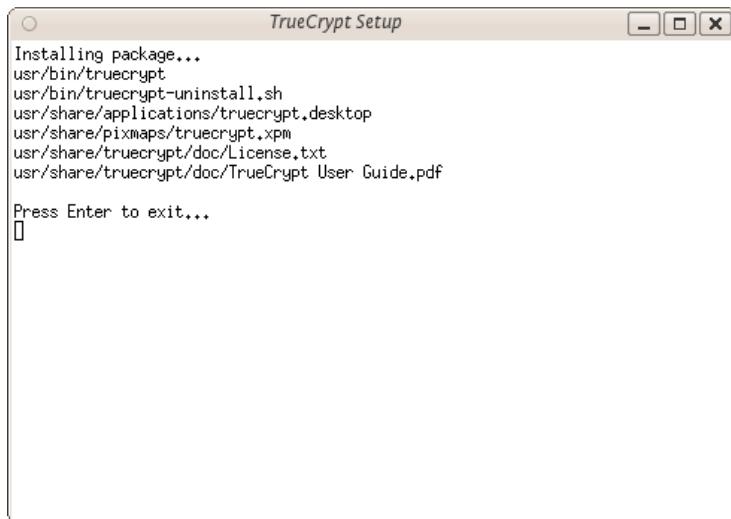


Figure 45.8: Instalación finalizada

---

## Instalación en OSX

1. Para instalar TrueCrypt en OSX primeramente visite la página de descarga y presione el botón de descarga en la sección OSX.

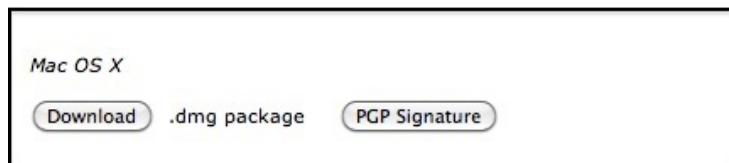


Figure 45.9: Página de descargas

2. Finalizada la descarga busque el archivo .dmg y ábralo para acceder al paquete de instalación
3. Abra el paquete de instalación, y presione en algún lugar del diálogo.
4. Elija la instalación estándar. (usted puede elegir una instalación personalizada y no seleccionar FUSE, pero no tiene sentido hacerlo. Lo necesita)
5. Terminada la instalación podrá hallar el programa en su carpeta de aplicaciones

## Instalación en Windows

Para instalar TrueCrypt en Windows primeramente visite la página de descarga (<http://www.truecrypt.org/downloads>) y presione el botón de descarga de la sección de Windows.

Descárguelo a su computadora y haga doble click en el archivo. Verá un acuerdo de usuario.

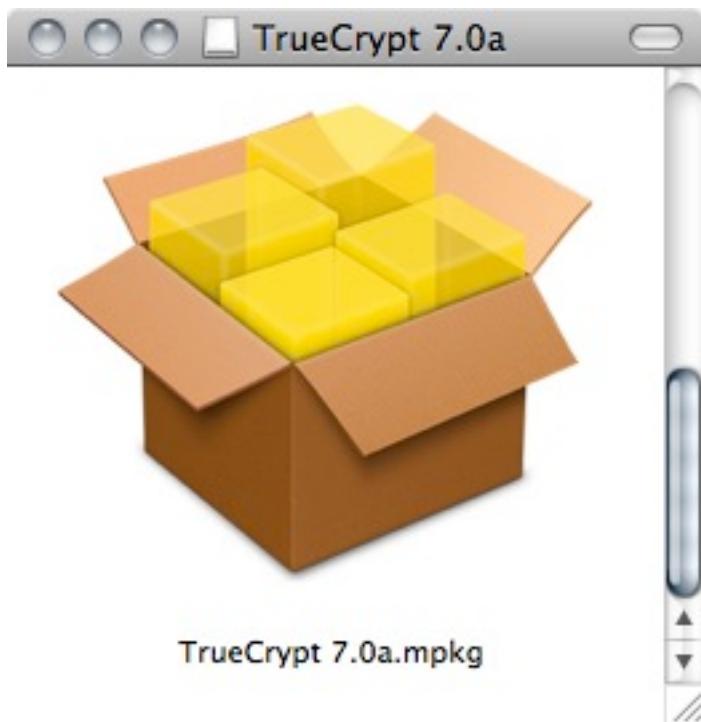


Figure 45.10: Abriendo el archivo

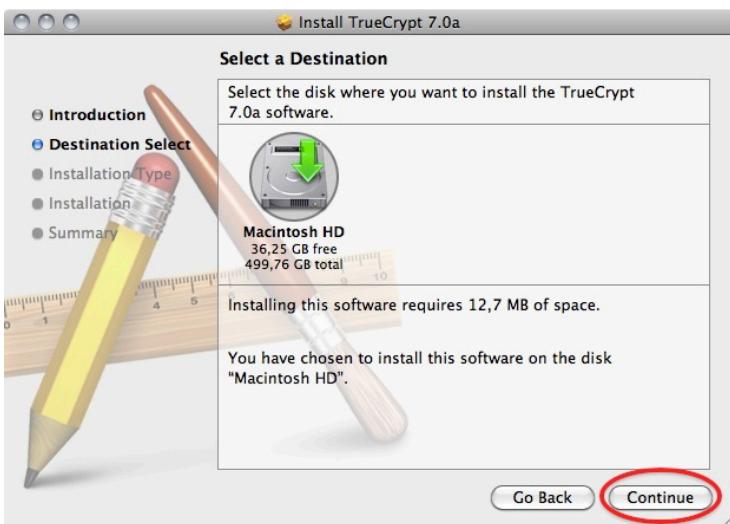


Figure 45.11: Abriendo el paquete de instalación

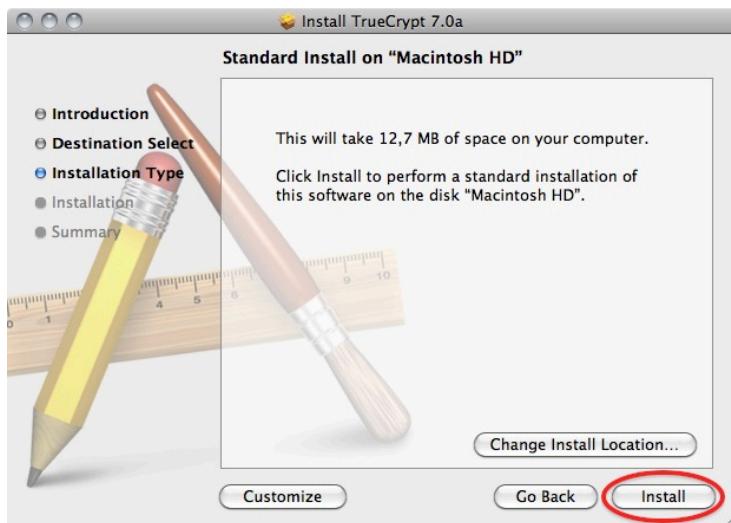


Figure 45.12: Instalando TrueCrypt



Figure 45.13: Instalación finalizada

Haga click en ‘I accept and agree to be bound by the license terms’ y presione ‘Accept’.

Salga de la pantalla anterior con los valores por defecto y presione ‘Next >’, aparecerá la ventana de opciones de configuración:

Puede dejar los valores predeterminados. Si desea instalar TrueCrypt sólo para usted, entonces no se recomienda seleccionar la opción “Instalar para todos los usuarios”. Sin embargo, si va a instalar esto en su propia máquina y nadie más usa la computadora, entonces esto no es necesario. Puede que también desee considerar la instalación de TrueCrypt en una carpeta distinta de la predeterminada. En este caso, haga clic en “Examinar” y elija otra ubicación. Cuando haya terminado, haga clic en “Instalar” y el proceso continuará:

Cuando se complete la instalación aparecerá una confirmación de se ha realizado correctamente. Cierre esta ventana y haga clic en “Finalizar”. Ahora continúe con el capítulo sobre el uso de TrueCrypt.

# 46

## Uso de TrueCrypt

Las siguientes instrucciones le indican paso a paso cómo crear, montar y usar un volumen TrueCrypt.

### Crear un contenedor TrueCrypt

1. Instale TrueCrypt. Luego ejecútelo mediante
  - haciendo doble click en el archivo TrueCrypt.exe en Windows
  - abriendo Aplicaciones->Accesorios->TrueCrypt en Ubuntu
  - abriéndolo en MacOSX haciendo click en Go > Applications. Busque TrueCrypt en la carpeta de aplicaciones y haga doble click en él.
2. Cuando aparezca la ventana principal de TrueCrypt seleccione Create Volume.
3. Aparecerá en pantalla el asistente de creación de volumen TrueCrypt.

## Uso de TrueCrypt

---

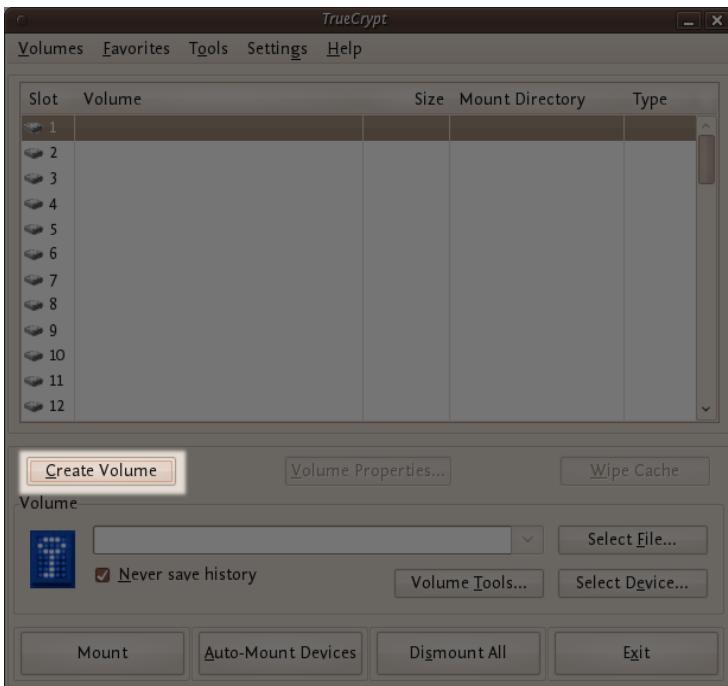


Figure 46.1: Creando un volumen



Figure 46.2: Asistente

Elija dónde crear el volumen TrueCrypt. Puede ser dentro de un archivo, que será llamado contenedor, en una partición o disco. Para lo siguiente supondremos que ha elegido la primera opción, crearlo dentro de un archivo.

Haga click en next

4. Ahora debe elegir crear un volumen estándar o uno oculto. Nosotros crearemos un volumen estándar.

Haga click en next

5. Ahora debe especificar el archivo contenedor del volumen TrueCrypt. Nótese que puede ser cualquiera, y podrá ser movido o borrado como cualquier archivo normal.

Haga click en Select File.

El selector de archivo estándar aparecerá en pantalla (el asistente permanece abierto por detrás). Ahora necesita navegar

## Uso de TrueCrypt

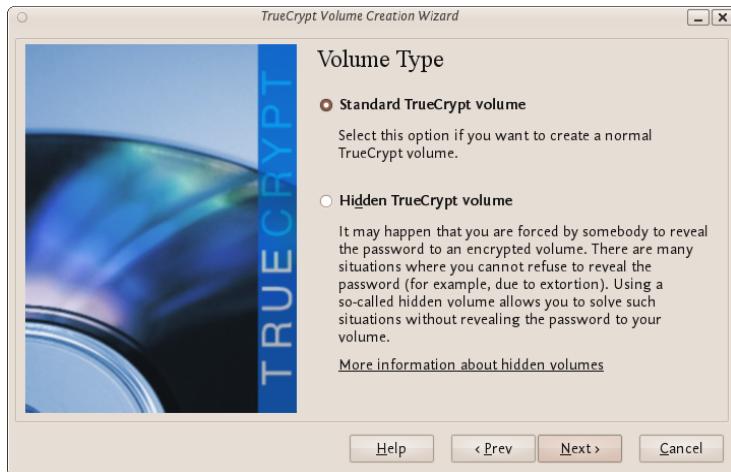


Figure 46.3: Tipo de volumen

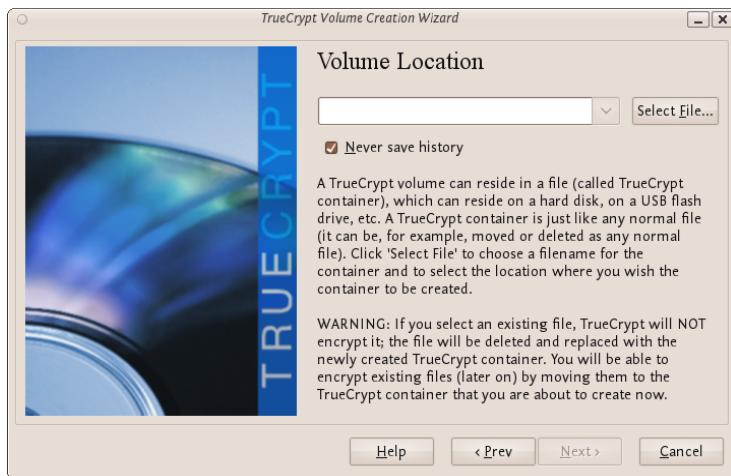


Figure 46.4: Archivo contenedor

---

hasta la carpeta que el archivo debería haber creado dentro entonces escriba en el campo ‘nombre’ el nombre del archivo que usted desea crear.

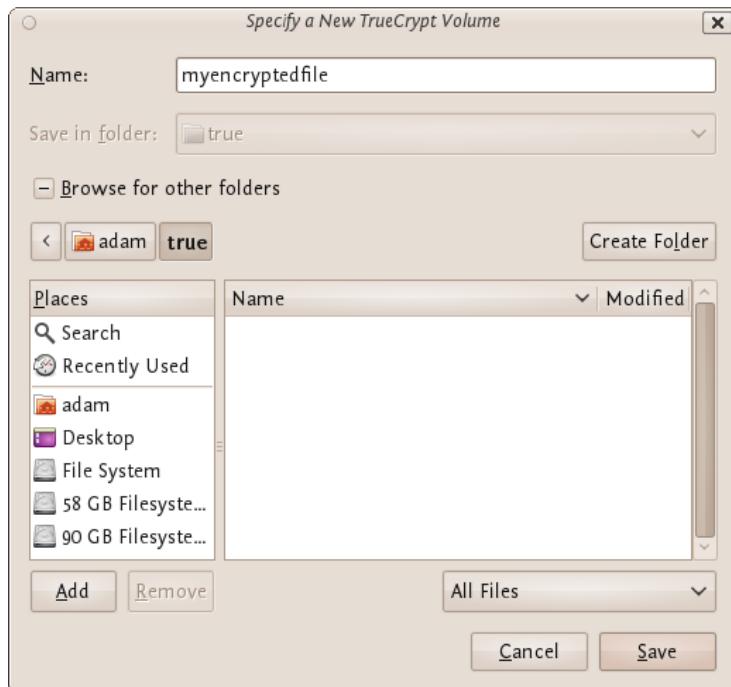


Figure 46.5: Escribiendo el nombre del archivo

Nosotros crearemos nuestro volumen TrueCrypt dentro de la carpeta ‘adam/true’ y el nombre del archivo del volumen (contenedor) será ‘myencryptedfile’. Usted puede, por supuesto, elegir cualquier otro archivo y cualquier otro soporte (por ejemplo, un pendrive). Observe que el archivo ‘myencryptedfile’ aún no existe - TrueCrypt lo creará. Presione ‘Save’ cuando esté listo.

La ventana de selección de archivo se cerrará.

**IMPORTANTE:** Note que TrueCrypt no cifrará ningún archivo existente. Si selecciona un archivo existente en este paso, será sobreescrito y reemplazado por el volumen creado (los datos se perderán). Podrá cifrar archivos existentes más tarde o moviéndolos al volumen TrueCrypt.

6. En la ventana del asistente de configuración (que estaba corriendo en el fondo) haga click en next.
7. Elija un algoritmo de cifrado y un algoritmo hash para el volumen.

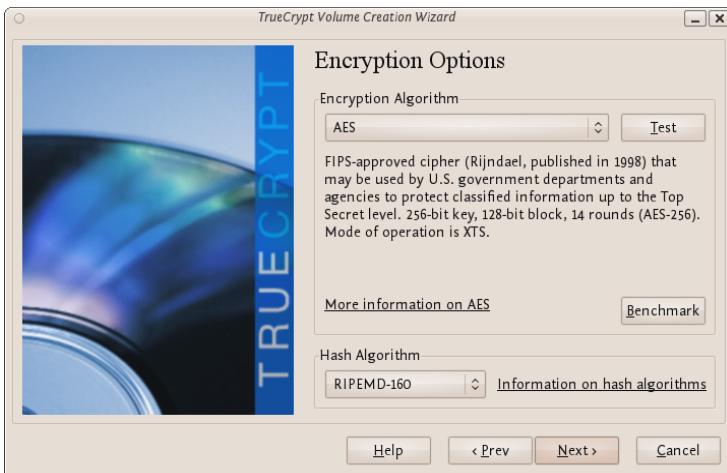


Figure 46.6: Selección del algoritmo de cifrado

El manual TrueCrypt sugiere que si usted no está seguro de su elección, utilice la configuración predeterminada y haga clic en Siguiente (para más información sobre cada ajuste echar un vistazo a la página web de documentación de TrueCrypt).

- 
8. Ahora elija el tamaño de su contenedor. Debería estar bien con 1 megabyte pero en el ejemplo nosotros ingresamos ‘20’.

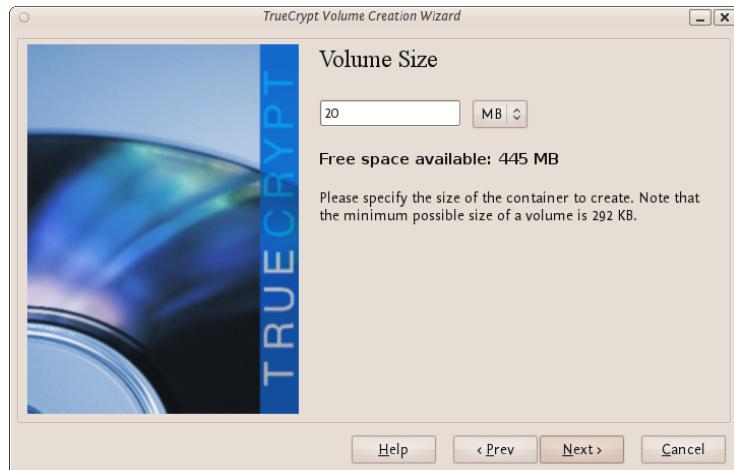


Figure 46.7: Fijando el tamaño del contenedor

Usted puede, por supuesto, especificar un tamaño diferente. Luego, haga click en next.

9. Este paso es realmente muy importante, elija una contraseña.

La información mostrada en la ventana del asistente le dirá si su contraseña es buena, debería leerla cuidadosamente.

Elija una contraseña fuerte, escríbala en el primer campo de entrada. Luego, repítala en el campo que está por debajo.

Presione entonces next.

10. Elija el formato de su partición (este paso no está disponible en Windows o OSX). Si usa Ubuntu puede

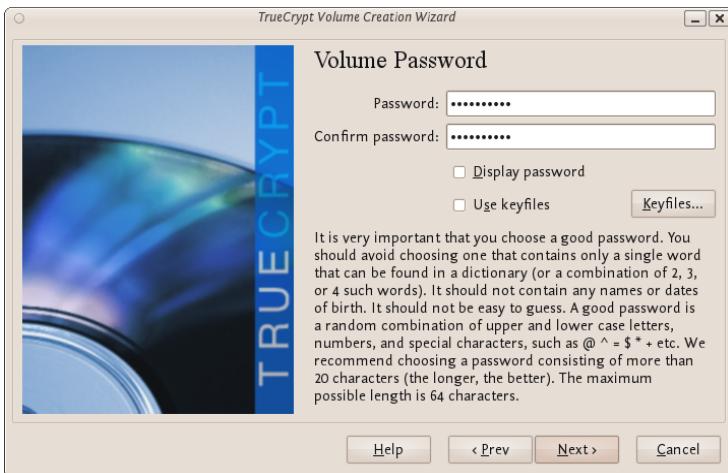


Figure 46.8: Estableciendo contraseñas

elegir un tipo de archivo GNU/linux o FAT (Windows) por simplicidad use la opción por default.

Luego presione next.

11. En este momento TrueCrypt intentará generar información aleatoria para poder cifrar su contenedor. Por un minuto mueva su ratón tan aleatoriamente como le sea posible. Esto aumenta considerablemente su seguridad incrementando la fortaleza criptográfica de su clave de cifrado.

Luego haga click en Format.

TrueCrypt ahora creará un archivo en la carpeta que usted eligió. Este archivo será un contenedor TrueCrypt, y contendrá un volumen TrueCrypt cifrado. Tomará algún tiempo dependiendo del tamaño del volumen. Cuando finalice debería aparecer:



Figure 46.9: Formato de la partición

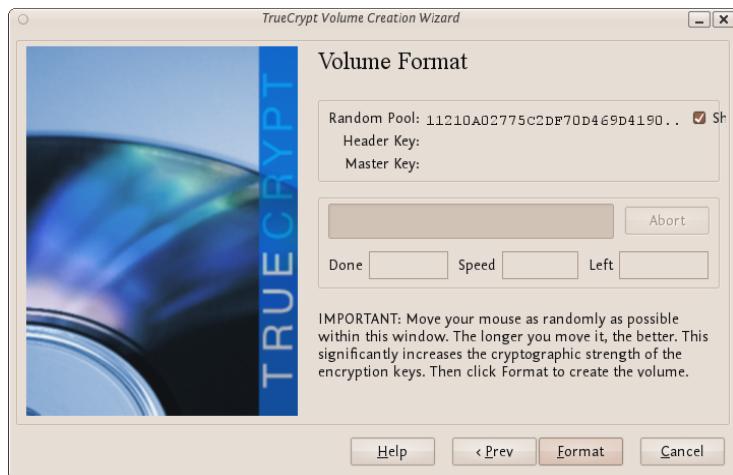


Figure 46.10: Cifrando el contenedor...

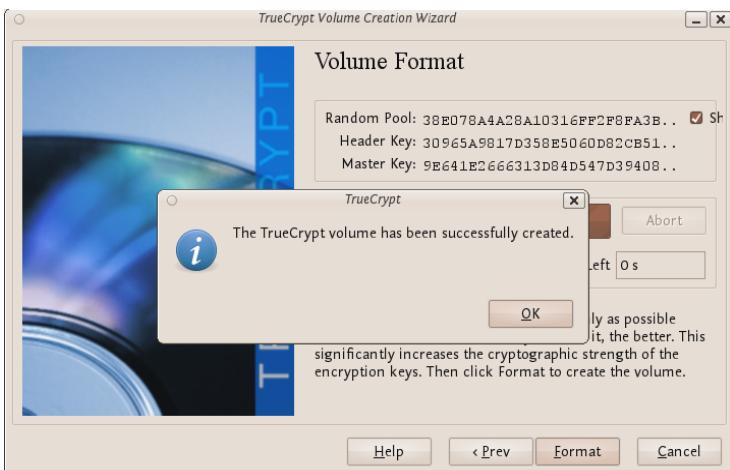


Figure 46.11: Cifrado terminado

Cierre la casilla de diálogos.

12. ¡Bien hecho! Ha creado satisfactoriamente un volumen TrueCrypt (archivo contenedor).

Cierre la ventana del asistente de creación de volúmenes TrueCrypt.

## Montando el volumen cifrado

1. Abra nuevamente TrueCrypt.
2. Asegúrese de elegir uno de los 'Slots' (no interesa cuál - puede optar por la opción por defecto, el primero de la lista). Haga click en Select File.

Aparecerá la ventana del selector de archivo estándar.

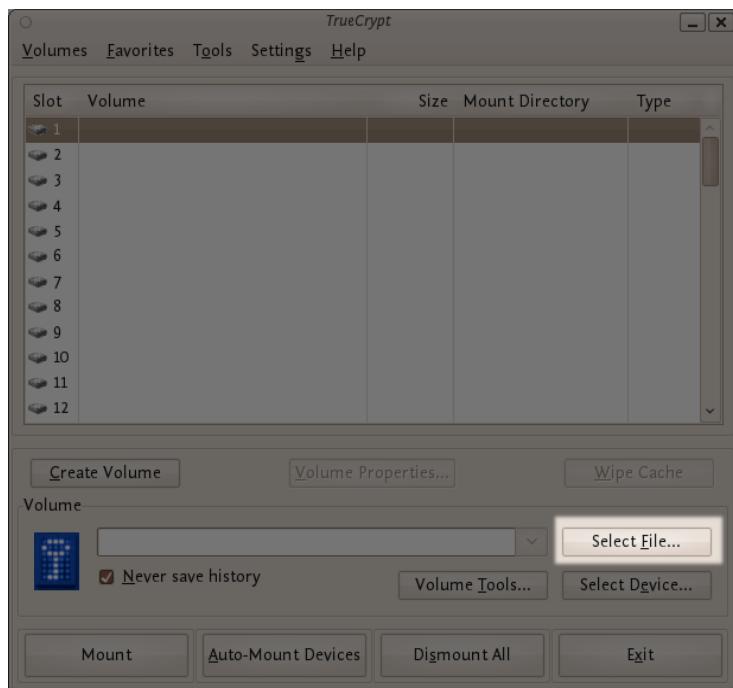


Figure 46.12: Eligiendo un slot

3. En el selector de archivo, navegue al archivo contenedor creado anteriormente y elíjalo.

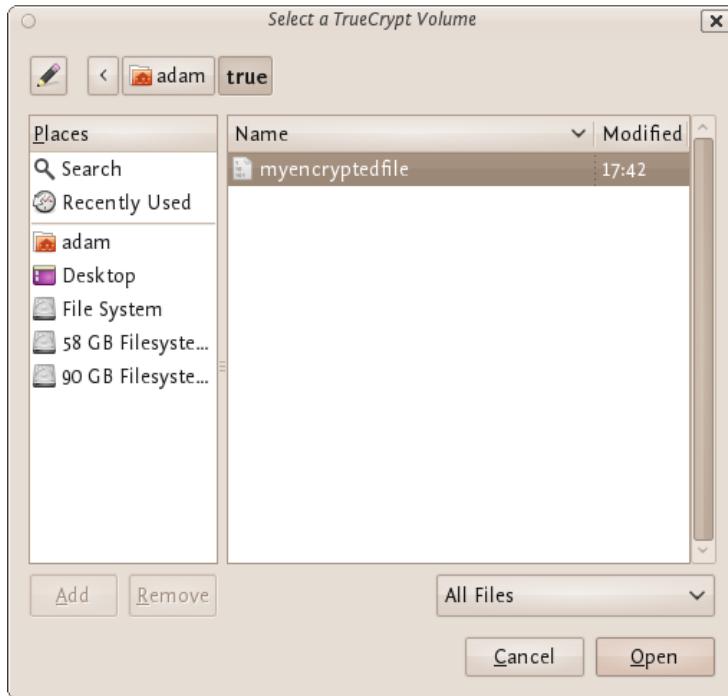


Figure 46.13: Selector de archivo

Haga click en Open (en la ventana del selector de archivo).

La ventana desaparecerá.

4. En la ventana principal de TrueCrypt, haga click en Mount.

Aparecerá una ventana de diálogo de la contraseña.



Figure 46.14: Montando el volumen

5. Ingrese su contraseña.
6. Presione OK para aceptar.

TrueCrypt procederá a montar el volumen si la contraseña es correcta.

Si la contraseña es incorrecta TrueCrypt le avisará y deberá repetir el paso anterior (tipar la contraseña y presionar OK).

7. Nosotros hemos montado exitosamente el contenedor como virtual disk 1. El contenedor aparecerá en su Escritorio o deberá buscarlo con su navegador de archivos.

## ¿Qué significa esto?

El disco que ha creado está completamente cifrado y se comporta como un disco real. Grabar (o mover, copiar, etc.) archivos en el disco le permitirá a usted cifrar archivos sobre la marcha.

Podrá abrir un archivo almacenado en un volumen TrueCrypt, el cual será descifrado automáticamente a la RAM mientras es

## Uso de TrueCrypt

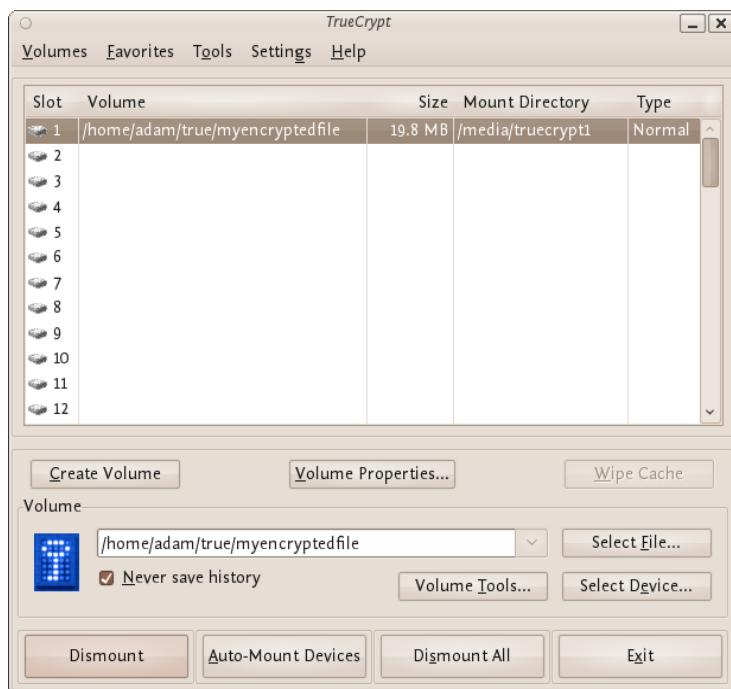


Figure 46.15: Ingresando la contraseña



Figure 46.16: Volumen montado

---

leído, y no necesitará ingresar su contraseña en cada ocasión. Solamente deberá ingresarla al montar el volumen.

## ¡Recuerde desmontarlo!

Haga click en el disco con el botón derecho y seleccione unmount. Esto sucederá automáticamente cuando apague su computadora pero no cuando se encuentre en modo suspendido. Configuración de un volumen oculto

---

Un volumen TrueCrypt oculto existe en el espacio libre de un volumen TrueCrypt típico. Suponiendo que accedamos al ‘volumen externo’, es (casi) imposible determinar si hay un volumen oculto dentro de él. Esto es así porque TrueCrypt *siempre* llena el espacio vacío de un volumen cifrado con datos aleatorios. Por eso un volumen oculto se ve igual que un volumen vacío.

Para crear y utilizar un volumen oculto se necesitan dos contraseñas - una para cada uno de los volúmenes, el exterior y el interior (oculto). Cuando monte (abra) el volumen puede utilizar cualquiera de ellos y esto determinará cuál de los dos estará abierto. Si desea abrir sólo el volumen oculto utilice una contraseña, y si usted desea tener acceso sólo al volumen cifrado no oculta deberá utilizar la otra contraseña.

Para crear un volumen abra TrueCrypt oculto y pulse el botón ‘Crear volumen’:

Las opciones para la mitad de este proceso son casi todas iguales a las usadas para configurar un volumen TrueCrypt estándar, no obstante indicaremos el proceso completo paso por paso. En la pantalla mostrada debajo deberá optar por la configuración por defecto ‘Create an encrypted file container’:

Presione ‘Next >’ y continúe a la próxima pantalla.

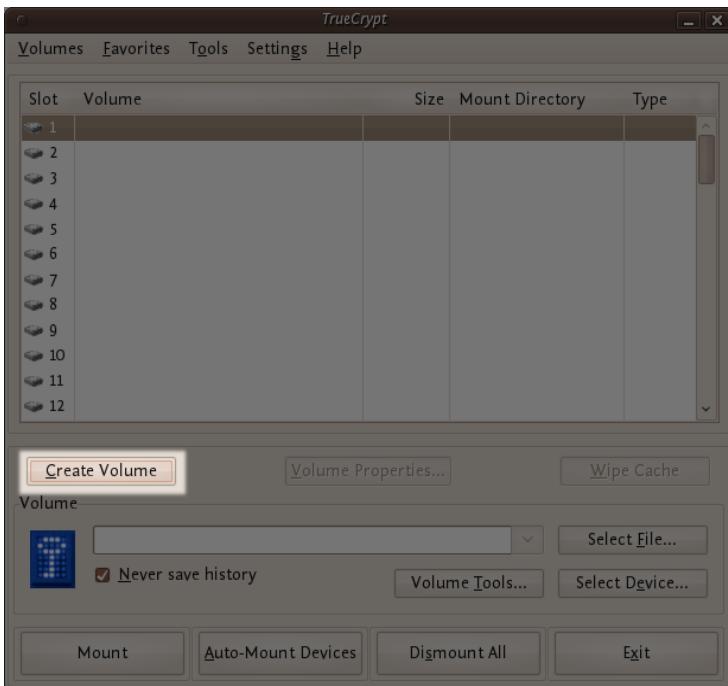


Figure 46.17: Creando un volumen oculto



Figure 46.18: Opciones de cifrado

Elija la segunda opción ‘Hidden TrueCrypt Volume’. Haga click en ‘Next >’ entonces le pedirán que seleccione un lugar y un nombre para el volumen TrueCrypt *externo*.

Haga click en ‘Select File...’ y navegue hasta el lugar donde ubicará el nuevo volumen. Nosotros usaremos el nombre ‘myencryptedfile’ en este ejemplo. Es el mismo nombre usado en el último ejemplo por eso tenga cuidado si ha seguido nuestras instrucciones anteriores porque ahora debe crear un volumen nuevo con un nombre diferente.

Navegue al directorio donde desea colocar el volumen externo e ingrese el nombre en el campo ‘Name’ como en el ejemplo anterior. Grabe los cambios. El navegador de archivos se cerrará y usted volverá al asistente. Presione ‘Next >’. Aquí se encontrará con algunas decisiones técnicas. No se preocupe. Acepte todas por defecto. La próxima pantalla le pedirá que determine

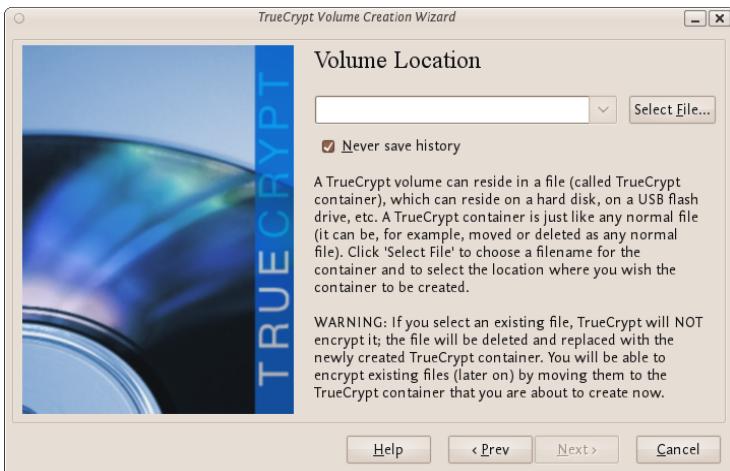


Figure 46.19: Seleccionando la ruta

el tamaño de su volumen externo. Note que cuando haga esto el tamaño máximo del volumen interior ‘oculto’ lo determina TrueCrypt. Este tamaño máximo será de hecho menor que el tamaño que usted está configurando en su pantalla. Si no está seguro de cuál es la relación entre el tamaño del volumen exterior y el tamaño del volumen interior (oculto) a partir de ahora deberá simular el proceso - siempre podrá desechar el volumen cifrado y empezar de nuevo (sin provocar ningún daño).

Elegimos entonces el tamaño del volumen exterior, que será de 20MB:

No se puede configurar el tamaño del volumen exterior más grande que el espacio libre disponible en su disco. TrueCrypt le informa el tamaño máximo posible en negrita. Luego haga clic en ‘Siguiente >’ y pasará a una pantalla que le solicitará que establezca una contraseña para el volumen exterior (no el

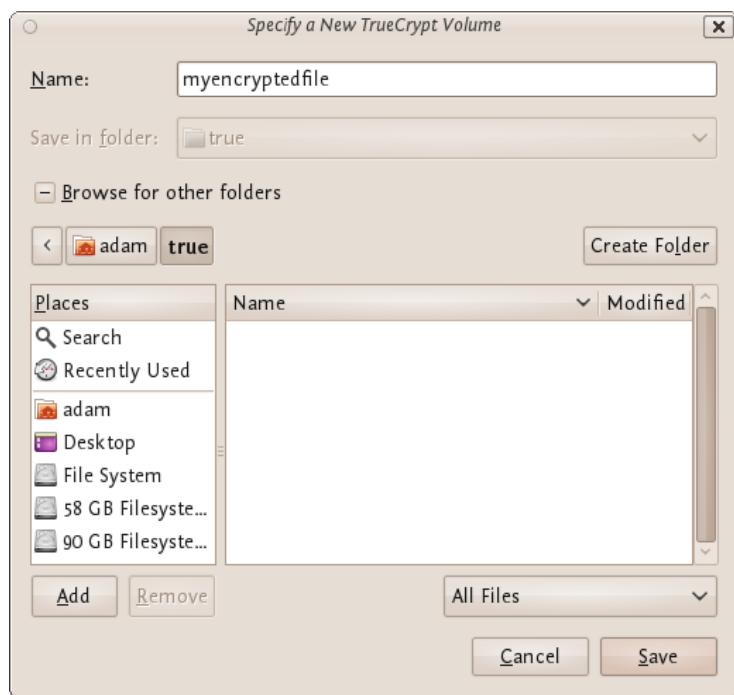


Figure 46.20: Eligiendo el nombre



Figure 46.21: Eligiendo el tamaño

oculto, esto viene después).

Ingrese una contraseña fuerte (consulte el capítulo acerca de crear buenas contraseñas) y presione 'Next >'. Ahora TrueCrypt lo ayudará a crear datos aleatorios para completar el volumen con ellos. Mueva zigzagueando su ratón por toda la pantalla, navegue por internet, haga cualquier cosa que se le ocurra. Cuando crea que TrueCrypt ya está satisfecho, pulse 'Format'. Usted verá una barra de progreso rápida y luego aparecerá la siguiente pantalla:

Usted puede abrir el volumen exterior si quiere, pero en este capítulo lo vamos a saltar y seguir adelante para crear el volumen oculto. Pulse 'Siguiente >' y TrueCrypt le informará el tamaño máximo posible del volumen oculto.

Cuando vea la pantalla mostrada más abajo, presione 'Next >'. Ahora podrá elegir el tipo de cifrado para el volumen oculto.

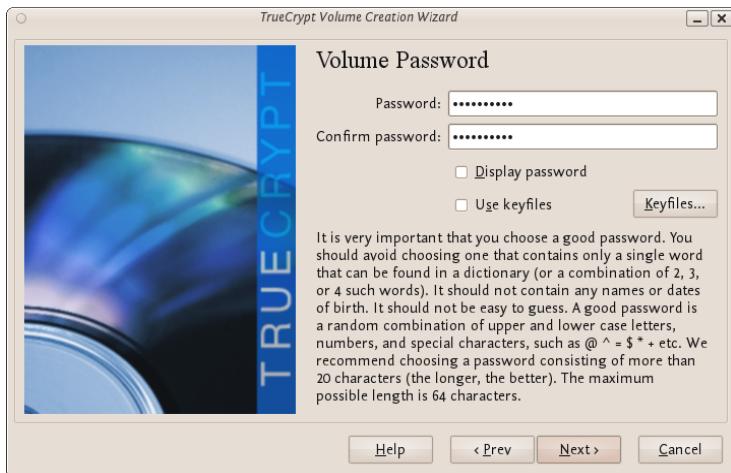


Figure 46.22: Estableciendo una contraseña

Mantenga el valor por defecto y presione 'Next >'.

Ahora le pedirá que le indique el tamaño del volumen oculto.

Nosotros hemos configurado (como puede ver más abajo) el tamaño máximo en 10MB. Cuando usted configure el suyo presione 'Next >' y podrá crear una contraseña para el volumen oculto.

Cuando cree la contraseña para el volumen oculto asegúrese que sea sustancialmente diferente de la contraseña del volumen exterior. Si alguien puede acceder a su disco y encuentra la contraseña del volumen oculto podría intentar ligeras variaciones de esta contraseña para ver si puede obtener también la contraseña del volumen oculto. Asegúrese que las dos contraseñas no son similares.

Ingrese su contraseña por duplicado y presione 'Next >'.

Mantenga los valores por defecto y presione ‘Next >’ entonces verá la misma pantalla que se le presentaba cuando generaba datos aleatorios para TrueCrypt. Cuando le dé la gana, presione ‘Format’ y verá lo siguiente :

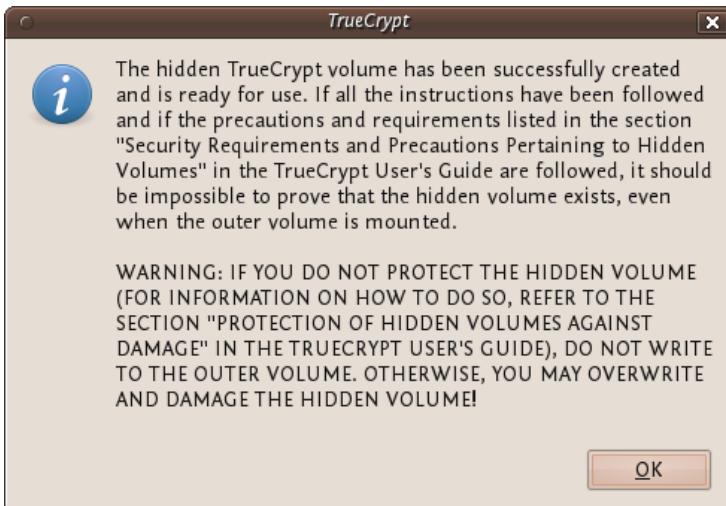


Figure 46.23: Dando formato

El manual de TrueCrypt al cual se refiere no es este, es el que se encuentra en <http://www.truecrypt.org/docs/>

Presione ‘OK’ y cierre TrueCrypt. Ahora puede montar el volumen como se describió en el capítulo anterior. Destrucción segura de datos =====

No crea que con presionar el botón delete todo estará hecho. No es tan sencillo. Para comprender cómo borrar datos en forma segura, debemos comprender cómo se almacenan. Haciendo una analogía con el mundo real, explicaremos el almacenamiento de datos como sigue:

---

Supongamos que usted posee una pequeña agenda con 10 páginas y quiere escribir algunos datos en ella. Comenzará a escribir a partir de la primera página. Puede ser que decida destruir la información de la página 5. Probablemente arranque la hoja y le prenda fuego.

Desafortunadamente los datos en un disco rígido no trabajan de la misma manera. Un disco rígido no contiene diez, sino miles o tal vez millones de páginas. También es imposible sacar una “página” y destruirla. Para explicar cómo trabaja un disco rígido, vamos a seguir con nuestro ejemplo de la agenda de 10 páginas. Pero ahora vamos a trabajar un poco diferente con ella. Vamos a trabajar de una manera similar a cómo funciona un disco rígido.

Esta vez usaremos la primera página como índice. Supongamos que escribimos un texto sobre “WikiLeaks”, entonces en la primera página escribiremos “texto sobre WikiLeaks: vea la página 2”. Entonces el texto se escribe luego en la página 2.

Para los próximos documentos, añadimos una línea en la página 1 referida a “Goldman Sachs”, “Goldman Sachs: vea la página 3”. Continuamos de esta forma hasta completar la agenda. Supongamos que la primera página resulta de la siguiente manera:

- WikiLeaks -> vea la página 2
- Goldman Sachs -> vea la página 3
- Monsanto scandal -> vea la página 4
- Holiday pictures -> vea la página 5
- KGB Investigation -> vea la página 6
- Al Jazeera contacts -> vea la página 7
- Iran nuclear program -> vea la página 8
- Sudan investigation -> vea la página 9
- Infiltration in EU-politics -> vea la página 10

Ahora, supongamos que decidimos borrar el documento “Gold-

man Sachs”, lo que el disco rígido va a hacer es eliminar sólo la entrada en la primera página, pero no los datos reales, el índice quedará así:

- WikiLeaks -> vea la página 2
- Monsanto scandal -> vea la página 4
- Holiday pictures -> vea la página 5
- KGB Investigation -> vea la página 6
- Al Jazeera contacts -> vea la página 7
- Iran nuclear program -> vea la página 8
- Sudan investigation -> vea la página 9
- Infiltration in EU-politics -> vea la página 10

Como eliminamos sólo la referencia al artículo, si abrimos la página 3, todavía podremos leer el documento acerca de Goldman Sachs. Esta es exactamente la manera en un disco rígido “borra” un archivo. Con algún software especializado todavía puede “recuperarse” de la página 3.

Para eliminar de forma segura los datos, se debe hacer lo siguiente:

1. Abrir la página del documento “Goldman Sachs” (página 3)
2. Usar un borrador para eliminar el artículo de la página
3. Eliminar la referencia en el índice de la página 1

Bueno, usted se sorprenderá por la similitud entre este ejemplo y el mundo real. Usted sabe que cuando usted borra el artículo con una goma de borrar, todavía es posible leer algo de él. El lápiz deja una huella en el papel debido a la presión sobre el papel y también quedará algo de grafito sin borrar. Pequeñas huellas así quedan en el papel. Si realmente necesita este artículo, se pueden reconstruir (partes) de él, aunque haya sido borrado.

Con un disco rígido la situación es muy similar. Incluso si se borra cada pieza de datos, a veces es posible recuperar parte

---

de estos datos usando un hardware (muy) especializado. Si los datos son muy confidenciales y deben ser borrados con el mayor cuidado, se puede utilizar software para “sobreescribir” todas las piezas de datos con datos aleatorios. Si se hace esto varias veces, será virtualmente imposible recuperar los datos.

## **Nota acerca de los discos rígidos de estado sólido**

Las siguientes instrucciones explican cómo utilizar las herramientas para eliminar archivos de forma segura de sus discos rígidos. Estas herramientas dependen de que el sistema operativo que esté utilizando sea capaz de direccionar directamente cada byte del disco rígido en forma ordenada para decirle “configure número de byte de X a 0”. Desafortunadamente, debido a una serie de tecnologías avanzadas utilizadas por unidades de estado sólido (SSD) como TRIM, no siempre es posible asegurar con 100% de certeza de que cada parte de un archivo en un disco SSD ha sido borrada usando las herramientas mostradas a continuación.

## **Borrado seguro de datos en Windows**

Para Windows existe una buena herramienta de código abierto llamado “File Shredder”. Esta herramienta se puede descargar desde <http://www.fileshredder.org>

La instalación es muy sencilla, sólo tiene que descargar la aplicación e instalarla pulsando el botón next una y otra vez. De spués de la instalación esta aplicación se iniciará automáticamente. A continuación, puede empezar a usarlo para borrar archivos. Sin embargo, la mejor parte del programa es que

## Uso de TrueCrypt

---

puedes usarlo desde dentro del propio Windows, haciendo click con el botón derecho sobre un archivo.

1. Haga click derecho en el archivo que desea borrar, y elija File Shredder -> Secure delete files

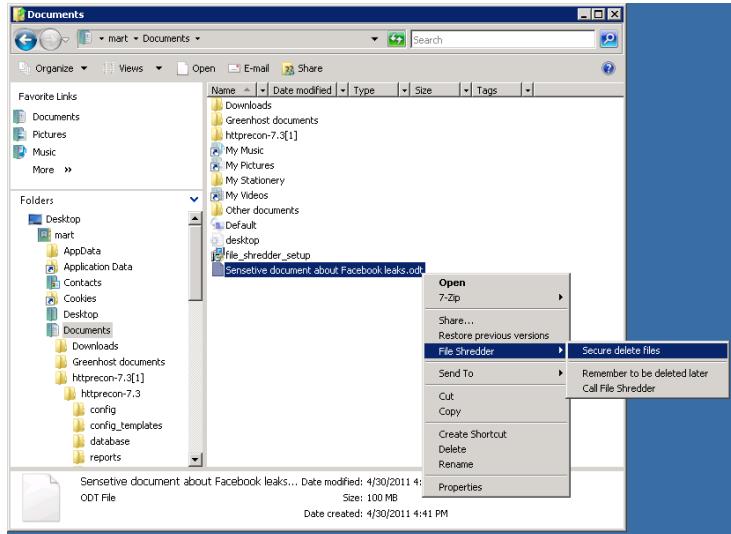


Figure 46.24: Borrado seguro

2. Un pop-up le preguntará si realmente desea borrar este archivo
3. Tras su confirmación, dependiendo del tamaño del archivo, el borrado tardará unos minutos

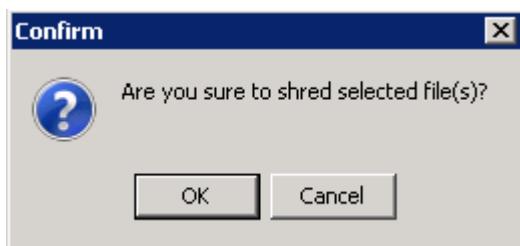


Figure 46.25: Confirmación del borrado



Figure 46.26: Borrando...

## Borrado seguro de datos en MacOSX

Siga los pasos siguientes para borrar datos en forma segura en su Mac OSX.

1. Borre el espacio libre en su disco rígido que contiene todos los datos de los ítem que fueron borrados en forma insegura.
2. Asegúrese de que todos los archivos a partir de ahora se eliminan siempre de forma segura.

Empecemos con el primer paso:

### Borrando el espacio libre

1. Abra la utilidad de disco la cual reside en la carpeta Utilities dentro de la carpeta Applications.
2. Seleccione su disco rígido y haga click en ‘Erase Free Space’.
3. Aparecerán tres opciones, aumentando la seguridad de arriba hacia abajo, pero también tardará mucho más tiempo en completarse. Lea las descripciones de cada uno de ellos para poder seleccionar lo que se adecúe mejor a sus necesidades y haga click en ‘Erase free Space’.

Si el tiempo no es un problema, use el método más seguro y disfrute de su tiempo libre para obtener un buen café mientras su Mac cruce con esta tarea. Si los ladrones ya están llamando a su puerta principal es posible que desee utilizar la forma más rápida.



Figure 46.27: Borrado del espacio libre

## Uso de TrueCrypt

---

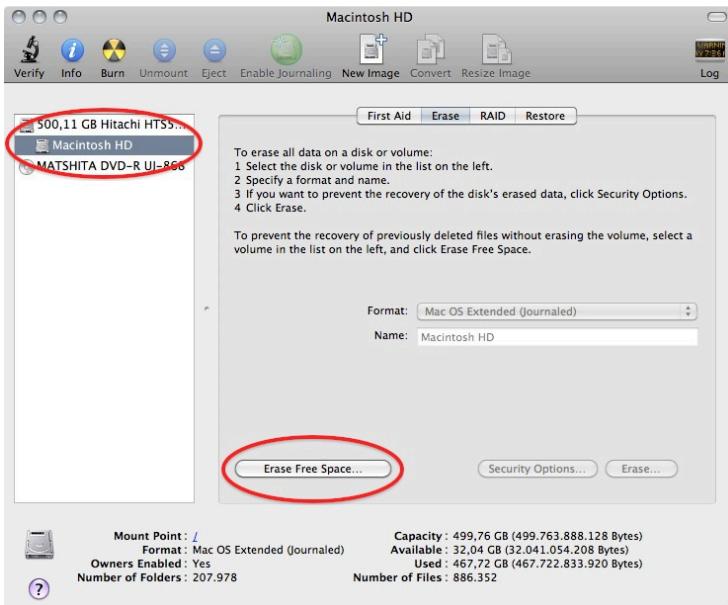


Figure 46.28: Confirmación del borrado

---

### Erase Free Space Options

These options write over the unused space on the selected disk or volume to prevent disk recovery applications from recovering deleted files.

Note: Secure Erase overwrites data accessible to Mac OS X. Certain types of media may retain data that Disk Utility cannot erase.

#### Zero Out Deleted Files

This provides good security and is quick. It writes zeros over the unused space in the disk once.

#### 7-Pass Erase of Deleted Files

This option provides better security and takes 7 times longer than "Zero Out Deleted Files." It writes over the unused space in the disk 7 times.

#### 35-Pass Erase of Deleted Files

This option provides the best security and takes 35 times longer than "Zero Out Deleted Files." It writes over the unused space in the disk 35 times.



Cancel

Erase Free Space

Figure 46.29: Selección del nmétodo de borrado

## Borrado seguro de archivos

Ahora que sus datos han sido eliminados para siempre debe asegurarse de que usted no creará nuevos datos que podrían ser recuperados en una fecha posterior.

1. Para hacer esto,abra el buscador de preferencias bajo el menú Finder.



Figure 46.30: Buscador de preferencias

2. Vaya a la pestaña advanced y marque 'Empty trash securely'. Esto le asegurará que cuando vacíe su papelera todos los items serán borrados en forma segura.

**Nota:** borrar sus archivos en forma segura tardará mucho



Figure 46.31: Borrando en forma segura

tiempo más tiempo que el borrado simple. Si tiene que borrar grandes porciones de datos sin importancia (por ejemplo su colección de películas y mp3) debería desmarcar esta opción.

## Borrado seguro de datos en Ubuntu

Desafortunadamente no existe en la actualidad una interfaz gráfica disponible en Ubuntu para borrar archivos en forma segura. Existen dos comandos disponibles:

- shred
- wipe

Shred está instalado en Ubuntu por defecto y puede borrar archivos simples. Wipe no está instalado por defecto pero puede instalarse fácilmente con el Ubuntu Software Center o mediante línea de comandos con `apt-get install wipe`. Wipe es un poco más seguro y una mejor opción.

Es posible acceder a estos programas fácilmente agregándolos como una opción de menú adicional.

1. Suponemos que está familiarizado con el Ubuntu Software Center. Para agregar la opción *securely wipe*, deberá instalar los programas *wipe* y *nautilus-actions*

Si estos dos programas están instalados siga con el paso siguiente. Si no es su caso, instálelos usando el Ubuntu Software Center o la línea de comandos tipeando `apt-get install nautilus-actions wipe`

2. Abra “Nautilus Actions Configuration” desde System -> Preferences menu
3. Agregaremos una nueva acción haciendo click en “create new action button”, la primera opción en la barra de herramientas

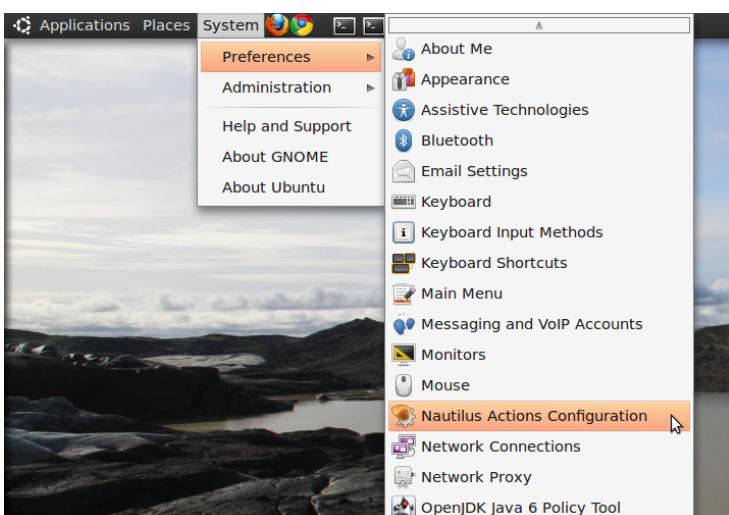


Figure 46.32: AConfigurando Nautilus

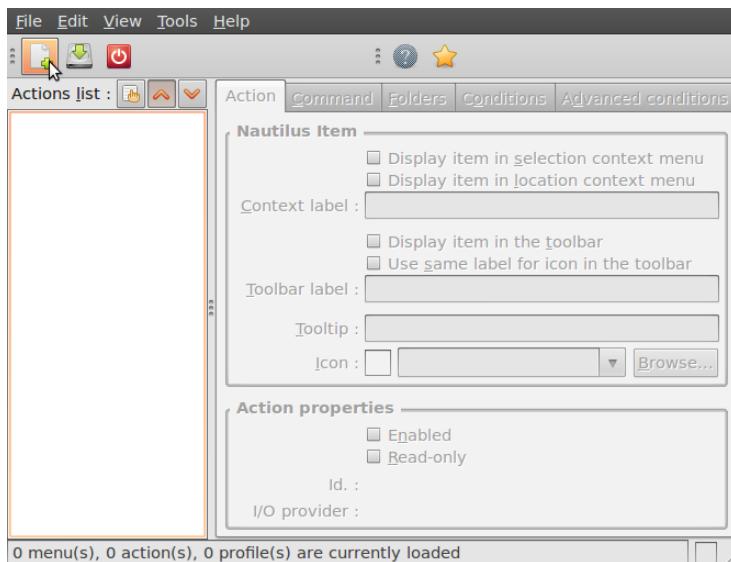


Figure 46.33: Creando una nueva acción

- 
4. Lo que sigue es describir la nueva acción. Puede darle a la acción el nombre que quiera. Colóquelo en el campo “Context label”. En este ejemplo usamos “Delete file securely”

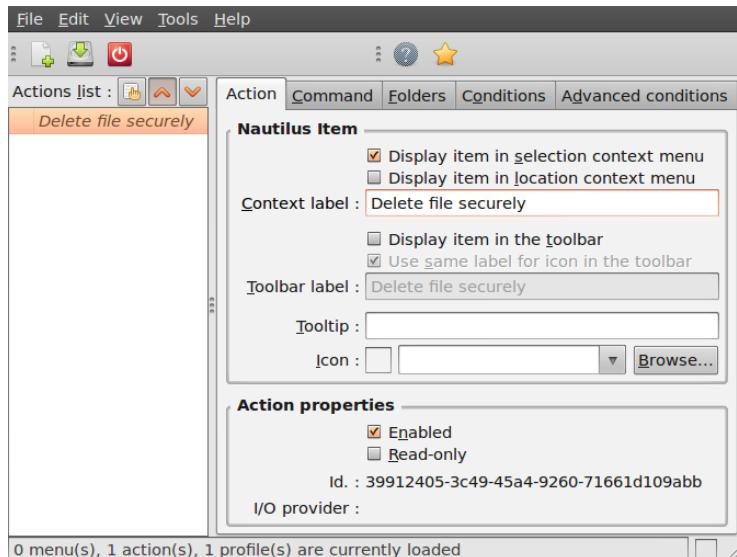


Figure 46.34: Describiendo la acción

5. Haga click en la segunda pestaña (“Command”), aquí especificaremos la acción que queremos realizar. En el campo “Path”, tipee “wipe”, en tipos de parámetro escriba “-rf %M”, asegúrese de hacerlo correctamente, es muy importante.
6. Especifiquemos las condiciones, haga click en la pestaña de condiciones y elija “Both” en la caja de diálogos “Appears if selection contains...”. Con esta opción podrá borrar archivos y carpetas en forma segura. Grabe los cam-

## Uso de TrueCrypt

---

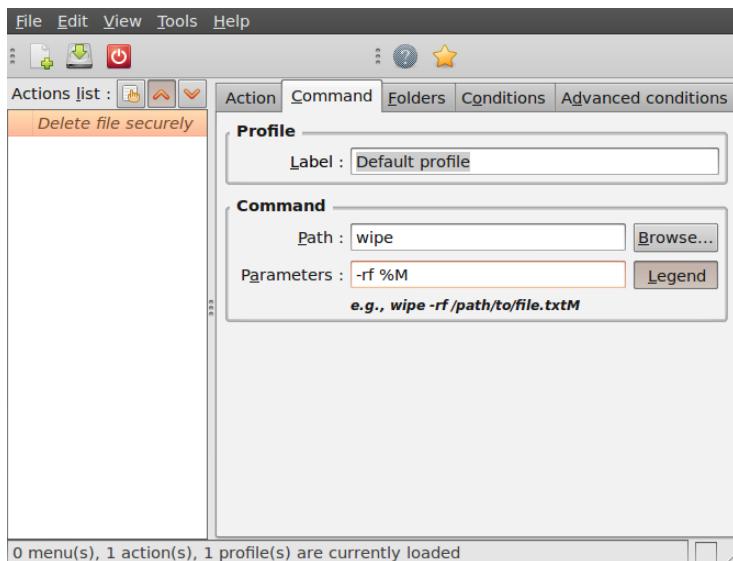


Figure 46.35: Configurando la acción

bios

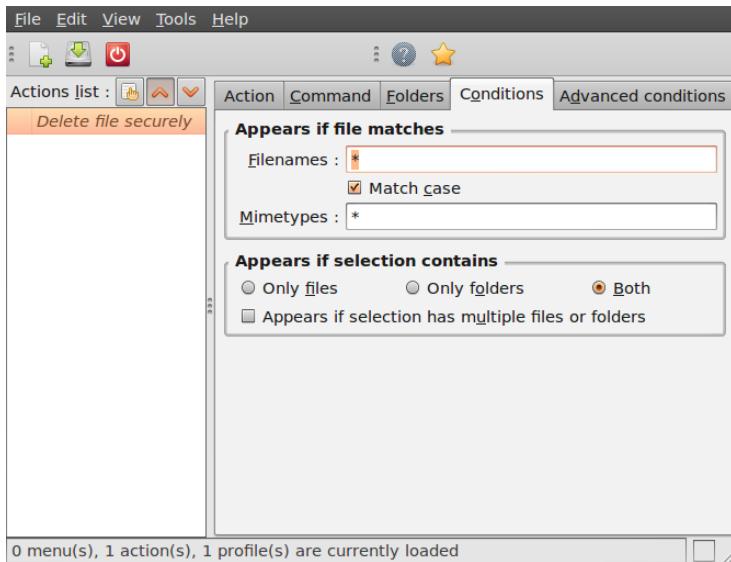


Figure 46.36: Terminando la configuración

7. Cierre la herramienta de configuración de acciones Nautilus. Tendrá que reiniciar su sesión para que los cambios surtan efecto.
8. Ahora navegue hasta el archivo que desea borrar en forma segura y haga un click derecho:

Elija ‘Delete File Securely’. El archivo será borrado ‘tranquilamente’ - no se dará cuenta que el proceso ha comenzado o ya concluyó. Sin embargo, el proceso está en marcha. Se necesita algún tiempo para eliminar de forma segura los datos y el más grande es el archivo que más tardará. Cuando se complete, el ícono del archivo a ser borrado desaparecerá. Si usted quisiera añadir algunos comentarios puede cambiar el campo de

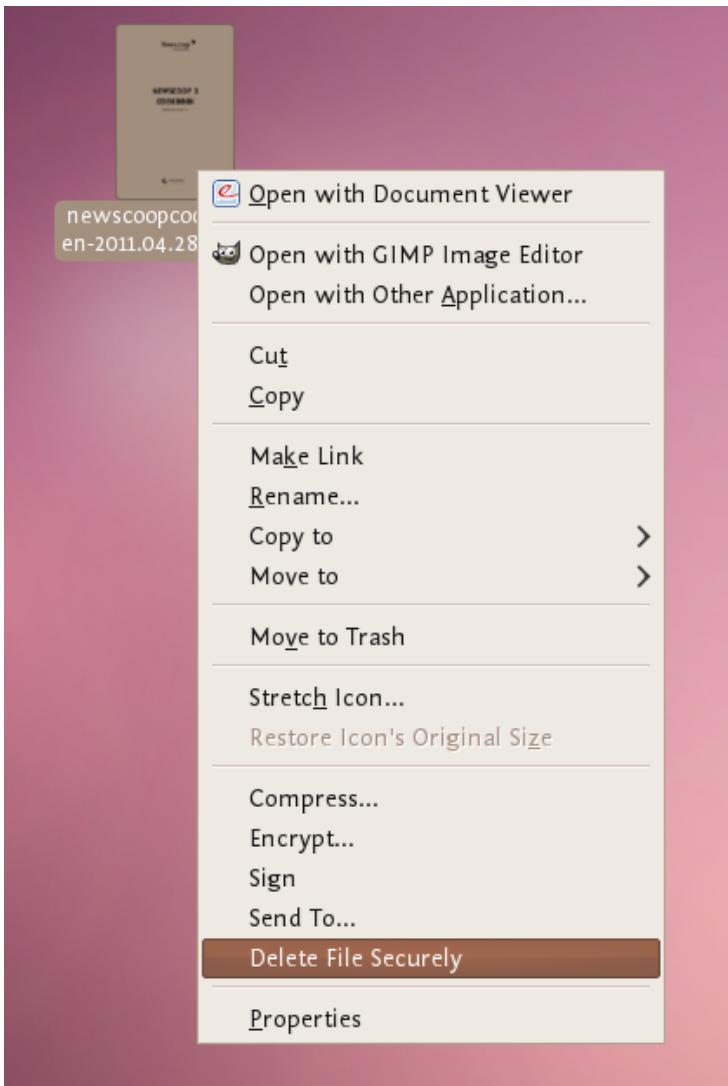


Figure 46.37: Borrando un archivo

---

los parámetros en la herramienta de configuración de acciones Nautilus, por ejemplo así:

```
-rf %M | zenity --info --text "your wipe is underway  
please be patient. The icon of the file to be wiped  
will disappear shortly."
```

La línea de arriba le indicará que el proceso está en marcha pero el archivo no será eliminado hasta que desaparezca el ícono.  
About LUKS =====

**LUKS**, short for *Linux Unified Key Setup*, is the default method for disk encryption on Linux. It can be used to enable *Full Disk Encryption* during installation with a single click, or to encrypt individual partitions on external hard disks or usb sticks later on. Please note that *Full Disk Encryption* is hard to enable **after** the installation as it requires moving all existing files temporarily as encrypting a device requires formatting it.

- Advantages: LUKS is available through dm-crypt which is part of the Linux kernel, so it doesn't need any further software to be installed.
- Disadvantages: Unlike with Truecrypt, it is not possible to use it with other Operating Systems (yet), so if you use LUKS to encrypt a USB drive, you can only use it on Linux machines, but not on Windows or Mac OS.

If you want to encrypt a device after the Linux installation completed, you can use the *Disk*s utility which can be found in most Linux distribution's *System Settings*.

## Starting *Disk*s

On Ubuntu, start *Disk*s by pressing the Windows key and A, typing “disks” and selecting the corresponding program as shown below:

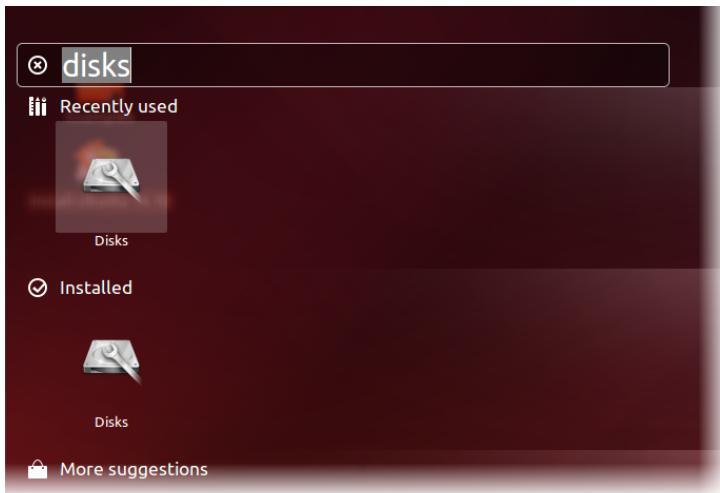


Figure 46.38: Launching Disks

---

# Encrypting a device

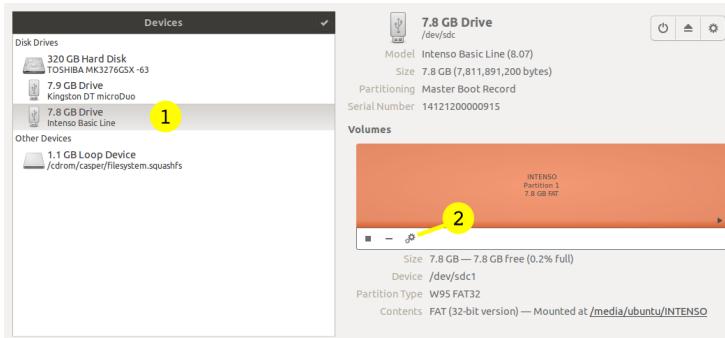


Figure 46.39: Disks main window

On the left hand side you will find a list of all storage devices plugged into your computer.

Select the one you want to encrypt (step 1) (in this case a usb stick), and then on the right hand side, click on the cog wheels and “Format...”. A dialog will appear where you can select if the existing data on the device shall be completely overwritten (that can take up to several hours depending on the size and performance of the device) or just formatted. Please note that even if you choose to encrypt the device, data, that was present before will be recoverable if you don't choose to overwrite it completely.

No matter what you choose for the field *Erase*, select “Encrypted, compatible with Linux systems (LUKS+Ext4)” for *Type*, give it a name and a strong passphrase (see chapter 8 on that matter), and click *Format...*

On the confirmation screen make sure you selected the correct device as data recovery is a cumbersome tasks – if possible at

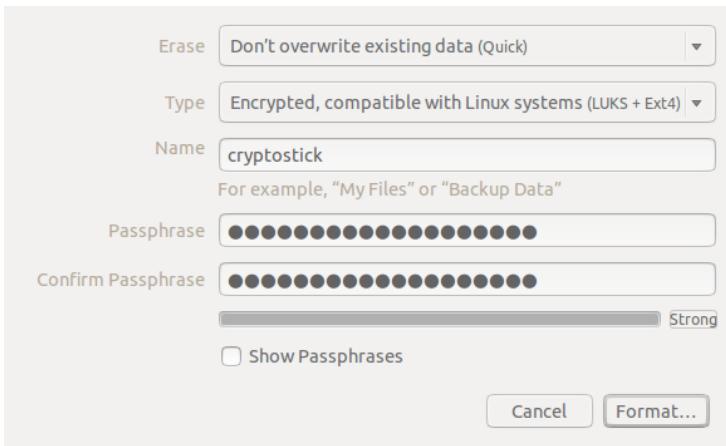


Figure 46.40: “Format...” dialog

all.

Back on the main window the device now consists of two layers. One is the physical storage (here called “Partition 1”) and the other a virtual device which is created by the LUKS system to give you access to the encrypted device (here called “cryptostick”). The pad lock on “Partition 1” is open as the *Disks* utility needed to open it in order to create a file system (how would you store files on a device without a file system?). You can click on the (other) pad lock as shown below to close the decryption channel and the *eject* button in the upper right corner to safely remove the device.

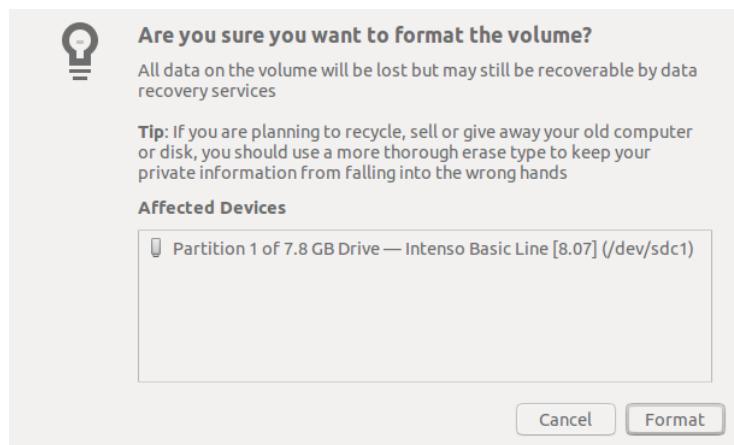
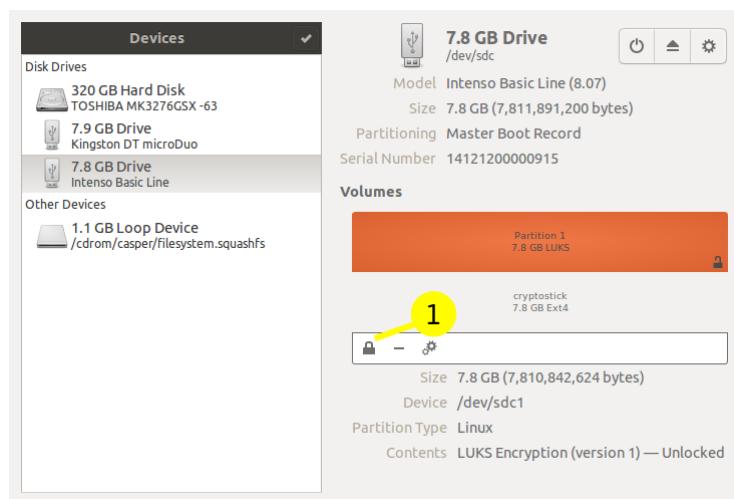
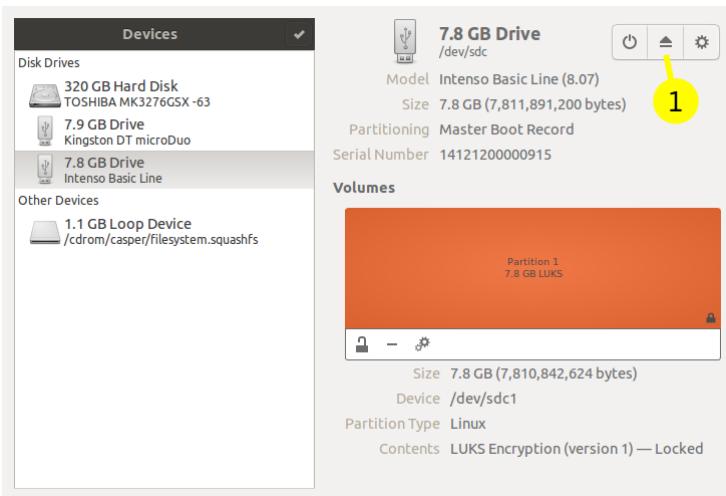


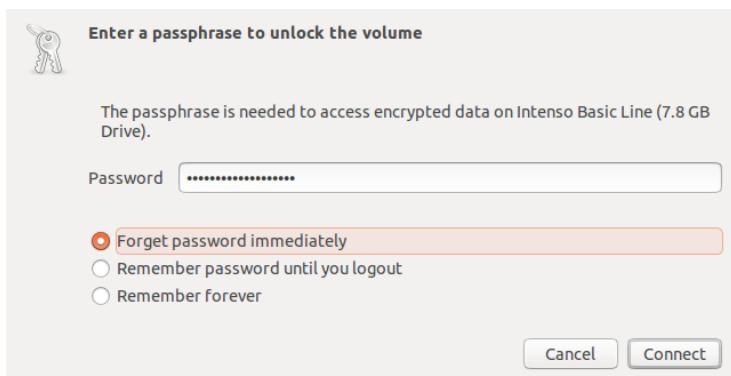
Figure 46.41: Confirmation step





## Using an encrypted device

This is quite straight-forward. Plug it in, enter the passphrase and click *Connect*. If the file manager does not open automatically, the device will be available when you do.



Instalación de CSipSimple =====

CSipSimple es un programa para dispositivos Android que permite hacer llamadas cifradas. Naturalmente, el software no es suficiente por sí solo y necesitamos una red de comunicación que nos permita hacer llamadas.

## Introducción a la red OSTN

Si conoce acerca de OSTN y tiene una cuenta, puede saltar esta sección.

La red de telefonía abierta (segura, de código abierto, estándar) OSTN del proyecto Guardian (<https://guardianproject.info/wiki/OSTN>) es un intento de definir una configuración estándar de voz sobre IP (VoIP) usando el protocolo de inicio de sesión SIP que permite llamadas cifradas de extremo a extremo. De manera similar al correo electrónico, SIP le permite a las personas elegir su proveedor de servicios sin perder su capacidad de llamar a los demás, incluso si no está utilizando el mismo proveedor. Sin embargo, no todos los proveedores de SIP ofrecen OSTN y los proveedores tienen que apoyar OSTN

para que las llamadas sean seguras. Una vez que una relación entre dos personas se ha establecido, los datos de audio se intercambian directamente entre las dos partes. Los datos se cifran de acuerdo con el protocolo de transporte seguro en tiempo real (SRTP).

La mayoría de las aplicaciones de cifrado de VoIP utilizan actualmente el protocolo de descripción de sesión denominado Descripciones de Seguridad para flujos de medios (SDES) con la seguridad de la capa de transporte (TLS) salto por salto para intercambiar claves maestras secretas para SRTP. Este método no es de extremo a extremo seguro como las claves de SRTP ya que son visibles en texto claro a cualquier proxy SIP o proveedor involucrado en la llamada.

Z RTP es un protocolo de acuerdo de clave cifrada para negociar las claves de cifrado entre dos partes. Los puntos extremos Z RTP utilizan el flujo de medios de comunicación en lugar del flujo de señalización para establecer las claves de cifrado SRTP. Puesto que la corriente de medios de comunicación es una conexión directa entre las partes que llaman, no hay manera para que los proveedores de SIP o proxies para interceptar las claves SRTP. Z RTP proporciona una tranquilidad razonable para los usuarios finales que tienen una línea segura. Al leer y comparar un par de palabras, los usuarios pueden estar seguros de que el intercambio de claves se ha completado.

## CSipSimple

CSipSimple es un cliente libre y open source para Android que trabaja bien con OSTN. Puede encontrarlo en <https://market.android.com/details?id=com.csipsimple>

Para usar CSipSimple con ostel.me, elija OSTN en el asistente genérico cuando cree una cuenta e ingrese un nombre de usuario,

---

contraseña y servidor según lo previsto después de inscribirse en Ostel

Una vez que llame a otra persona con CSipSimple aparecerá una barra amarilla con ZRTP y el par de verificación de palabra. Ahora se ha establecido una conexión de voz segura que no puede ser interceptada. Sin embargo, usted debe ser consciente de que el teléfono o el teléfono de la otra parte pueden estar configurados para grabar la conversación.

Pasos básicos:

1. Instalar CSipSimple desde Google Play store u otra fuente verificada
2. Ponerlo en marcha y elegir si desea realizar llamadas SIP a través de conexión de datos o sólo Wi-Fi
3. Configurar su cuenta

Para usar CSipSimple con ostel.me, elija OSTN en la sección Generic Wizards cuando cree una cuenta. Puede alternar entre los proveedores de los “Estados Unidos” haciendo clic en “Estados Unidos”. Ahora seleccione *OSTN*:

Ahora puede ingresar su usuario (número), contraseña y servidor (ostel.me) según lo previsto después de inscribirse en Ostel.

Ahora usted puede hacer una llamada. La primera vez que se conecte a una persona con ZRTP usted tiene que comprobar que el intercambio de claves se ha realizado correctamente. En el siguiente ejemplo la palabra de confirmación es “cieh”, usted puede hablar con la otra parte, y asegurarse de que ambos ven la misma palabra. Una vez terminado, pulse Aceptar.

Usted ha establecido una conexión de voz segura que no puede ser interceptada. Tenga en cuenta que usted o el teléfono de la otra parte podría estar grabando la conversación.

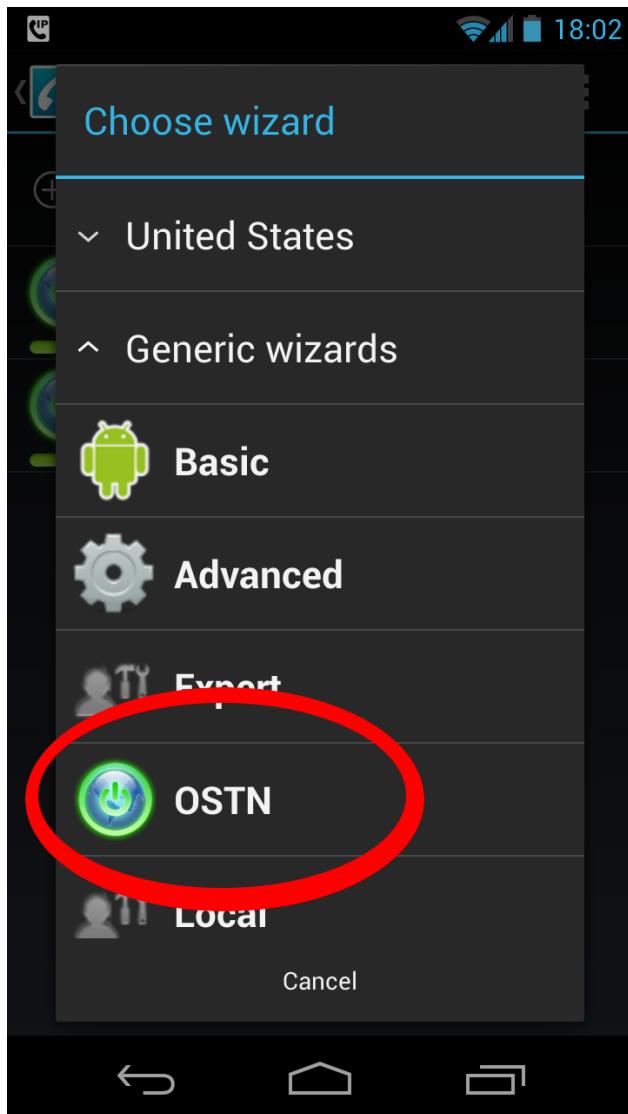


Figure 4642: OSTN

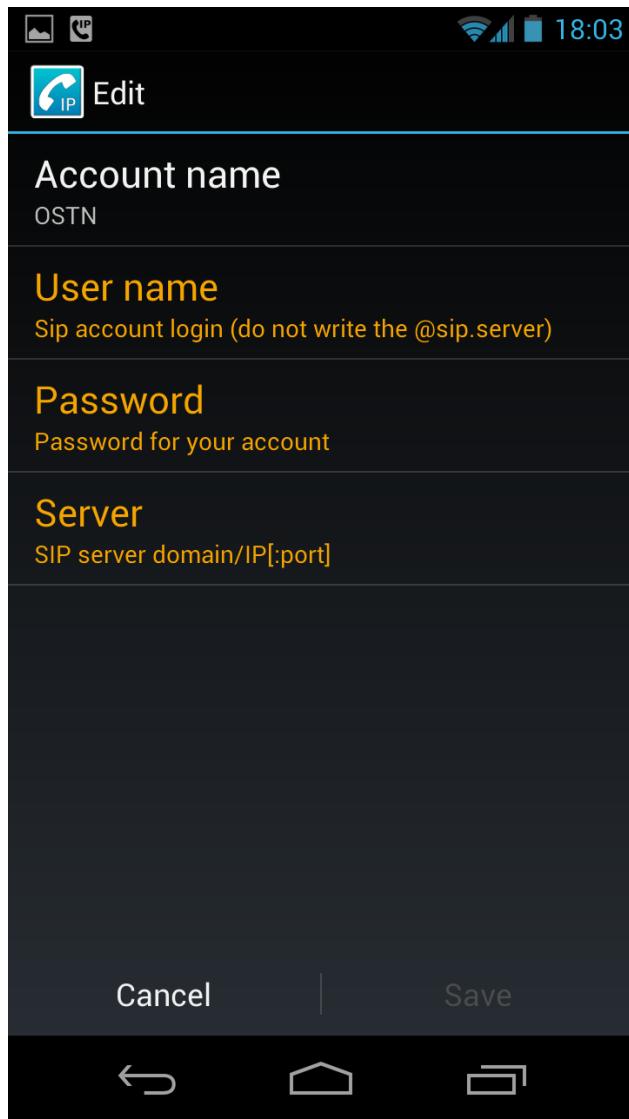


Figure 46.43: OSTN

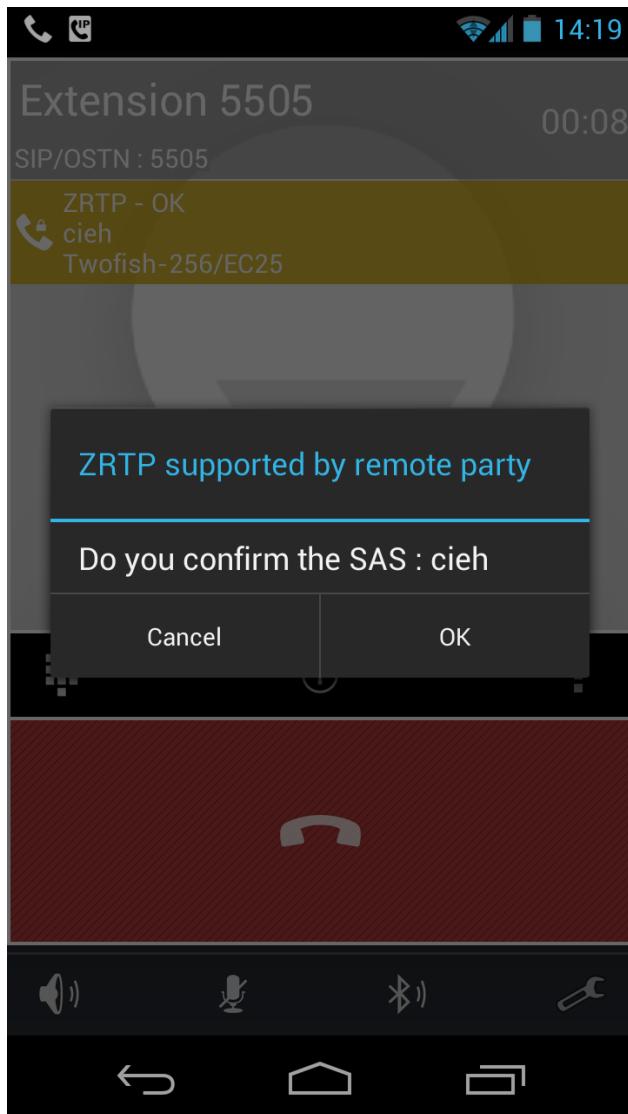


Figure 4644: OSTN

# 47

## Configuración de mensajería instantánea cifrada

### **Android - Instalación de Gibberbot**

<https://guardianproject.info/apps/gibber/>

Gibberbot es un cliente de chat seguro capaz de cifrado de extremo a extremo. Funciona con Google, Facebook, y Jabber o cualquier servidor XMPP. Gibberbot usa cifrado Off-The-Record estándar (OTR) para habilitar comunicaciones cifradas extremo a extremo verificables verdaderas.

Usted puede instalar Gibberbot a través del Google Play o a partir de otras fuentes autenticadas.

También puede chatear en forma segura con otros programas con soporte OTR tales como Adium, Pidgin en la computadora, Gibberbot en Android o ChatSecure en iOS.

## iOS - Instalación de ChatSecure

<http://chrisballinger.info/apps/chatsecure/>

ChatSecure es un cliente de chat seguro capaz de cifrar de extremo a extremo. Funciona con Google, Facebook y Jabber o cualquier servidor XMPP. ChatSecure usa cifrado estándar Off-the-Record (OTR) para habilitar las comunicaciones cifradas de extremo a extremo verificables verdaderas.

Puede instalar ChatSecure desde iTunes store.

Puede chatear en forma segura con otros programas con soporte OTR tales como Adium, Pidgin en la computadora, Gibberbot en Android o ChatSecure en iOS.

## Ubuntu - Instalación de Pidgin

<http://pidgin.im/>

Pidgin es un cliente de chat seguro capaz de cifrar de extremo a extremo. Funciona con Google, Facebook, Jabber o cualquier servidor XMPP. Pidgin utiliza el cifrado estándar Off-the-Record (OTR) para habilitar las comunicaciones cifradas de extremo a extremo verificables verdaderas.

Puede instalarlo desde el Ubuntu Software Center, busque pidgin-otr para instalar pidgin y el plugin otr.

Una vez instalado puede habilitar otr para cualquier cuenta que configure en pidgin.

Puede chatear en forma segura con otros programas con soporte OTR tales como Adium, Pidgin en la computadora, Gibberbot en Android o ChatSecure en iOS.

---

## OS X - Instalación de Adium

<http://www.adium.im/>

Adium es un cliente de chat seguro capaz de cifrado de extremo a extremo. Funciona con Google, Facebook, Jabber o cualquier servidor XMPP. Adium utiliza el cifrado estándar Off-the-Record (OTR) para habilitar las comunicaciones cifradas de extremo a extremo verificables verdaderas.

La instalación de Adium es similar a la instalación de la mayoría de las aplicaciones de Mac OS X.

1. Descargar la imagen de disco de Adium <http://www.adium.im/>.
2. Si una ventana Adium no se abre automáticamente, haga doble click en el archivo descargado
3. Arrastre la aplicación Adium a la carpeta Aplicaciones.
4. “Expulse” la imagen de disco Adium, que tiene un ícono de un disco
5. La imagen de disco Adium todavía estará presente en la carpeta de descarga (probablemente en el escritorio). Puede arrastrar el archivo a la papelera, ya que ya no es necesaria.
6. Para cargar Adium, colóquela en la carpeta Aplicaciones y haga doble click.

Puede chatear en forma segura con otros programas con soporte OTR tales como Adium, Pidgin en la computadora, Gibberbot en Android o ChatSecure en iOS.

## Windows - Instalación de Pidgin

<http://pidgin.im/>

Pidgin es un cliente de chat seguro capaz de cifrado de extremo a extremo. Funciona con Google, Facebook, Jabber o cualquier servidor XMPP. Pidgin utiliza el cifrado estándar Off-the-Record (OTR) para habilitar las comunicaciones cifradas de extremo a extremo verificables verdaderas.

Para utilizar Pidgin con OTR en Windows, es necesario instalar el plugin de Pidgin y OTR para Pidgin.

1. Descargue la última versión de Pidgin para Windows desde <http://www.pidgin.im/download/windows/>
2. Ejecute el instalador de Pidgin
3. Descargue la versión más reciente del “plugin OTR para Pidgin” de <http://www.cypherpunks.ca/otr/#downloads>
4. Ejecute el Instalador de Complementos OTR

Una vez instalado puede habilitar otr para cualquier cuenta que configure en pidgin.

Puede chatear en forma segura con otros programas con soporte OTR tales como Adium, Pidgin en la computadora, Gibberbot en Android o ChatSecure en iOS.

## Todos los OS - crypto.cat

<https://crypto.cat>

Cryptocat es una aplicación web de código abierto destinado a permitir chat online de forma segura y cifrada. Cryptocat cifra los chats en el lado del cliente, sólo confía en el servidor con los datos que ya están cifrados. Cryptocat se entrega como una extensión del navegador y ofrece plugins para Google Chrome, Mozilla Firefox y Apple Safari.

Cryptocat tiene la intención de proporcionar medios para las comunicaciones cifradas improvisadas, que ofrecen más privacidad que servicios como Google Talk, manteniendo al mismo tiempo

---

un mayor nivel de accesibilidad que otras plataformas de cifrado de alto nivel, y además permite múltiples usuarios en una sala de chat.

## Archivos de registros de chat

Algunos de los clientes de chat antes mencionados, por ejemplo, Adium, almacenan texto plano, sin cifrar los registros de chat, a menudo de forma predeterminada, incluso aún cuando está instalado el plugin de “seguridad/privacidad” OTR.

Si usted está tomando precauciones OTR para proteger sus sesiones de chat de fisgones a través en el cable o inalámbricos, debería comprobar que se ha apagado manualmente el Inicio de sesión de Chat, o asegurarse de que el registros de chat destinados deliberadamente para ser guardados son creados en un disco o volumen cifrado, en caso de que su equipo se pierda, sea robado o decomisado. También vale la pena preguntarle a la persona con la que está conversando si está registrando inadvertidamente el contenido de la charla con su propio software cliente de chat. Instalación de I2P on Ubuntu Lucid Lynx (y posteriores) y sus derivados como Linux Mint & Trisquel

---

1. Abra una terminal y escriba:

```
sudo apt-add-repository ppa:i2p-maintainers/i2p
```

Este comando agregará el PPA a /etc/apt/sources.list.d y descargará la clave gpg con la cual se ha firmado el repositorio. La clave GPG se asegura de que los paquetes no se han alterado desde que fue construido.

2. Notifique a su administrador de paquetes del nuevo PPA ingresando

```
sudo apt-get update
```

Este comando recuperará la lista más reciente de software de cada repositorio que está habilitado en el sistema, incluyendo el PPA I2P que se ha añadido con el comando anterior.

3. Ahora está listo para instalar I2P

```
sudo apt-get install i2p
```

4. Su explorador debería abrir con la consola del router I2P local, para navegar por dominios I2P tiene que configurar su navegador para usar el proxy I2P. También puede ver el estado de conexión en el lado izquierdo de la consola del router. Si su estado es **Network: Firewalled** su conexión va a ser bastante lenta. La primera vez que inicie I2P puede tardar algunos minutos para integrarse en la red y encontrar pares adicionales para optimizar su integración, por lo que por favor sea paciente.

En el menú Tools, seleccione Options para abrir el panel de configuración de Firefox. Haga click en el icono con la etiqueta Advanced, haga clic en la ficha Network. En la sección Connections, haga clic en el botón Settings. Verá una ventana como la siguiente:

En la ventana de Connection Settings, haga click en el círculo cercano a Manual proxy configuration, luego ingrese 127.0.0.1, port 4444 en el campo HTTP Proxy. Ingrese 127.0.0.1, port 4445 en el campo SSL Proxy. Asegúrese de ingresar localhost y 127.0.0.1 en la casilla de “No Proxy for”.

Para más información y cómo configurar proxies para otros navegadores consulte <https://www.i2p2.de/htproxyports.htm>

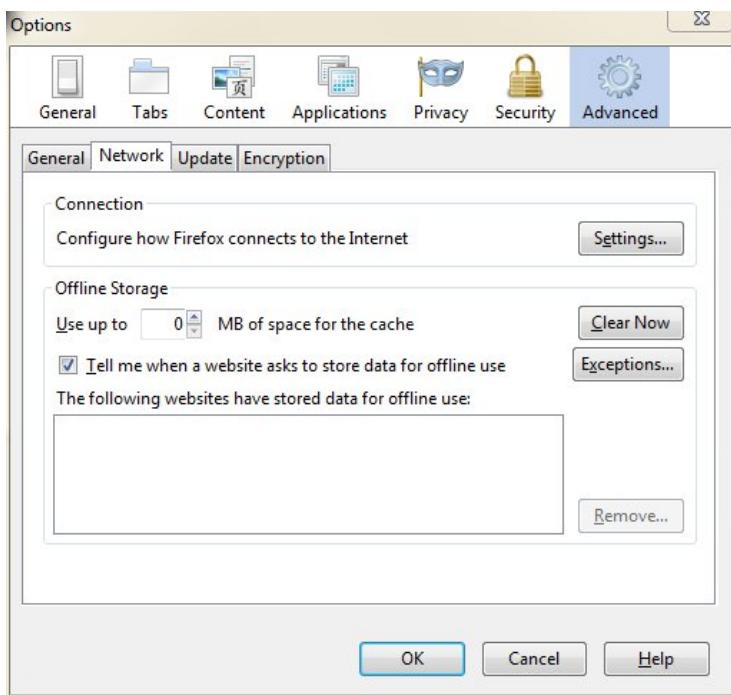


Figure 47.1: I2P

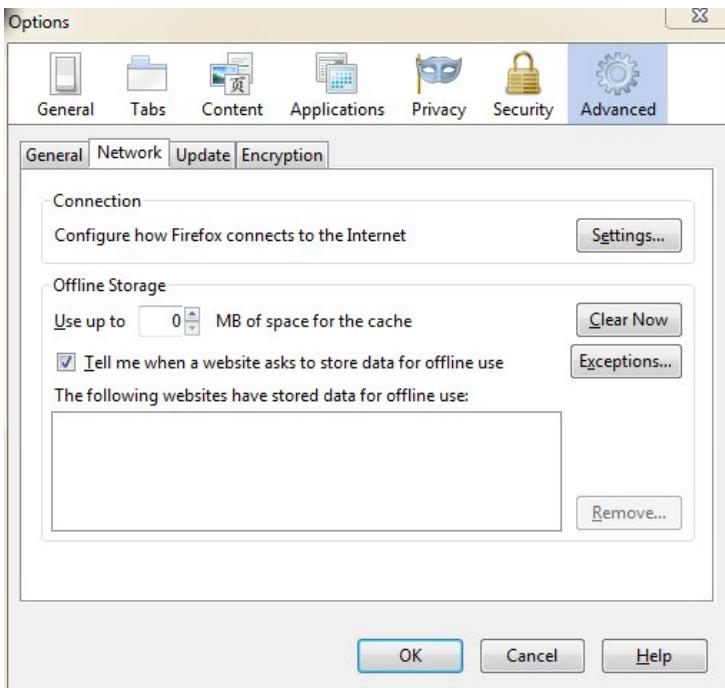


Figure 47.2: I2P

# 48

## Instrucciones para Debian Lenny y posteriores

Para más información visita esta página <https://www.i2p2.de/debian.html>



# 49

## Empezando con I2P

Usando estos paquetes I2P el router I2P puede iniciar de alguna de las siguientes formas:

- “on demand” usando el script i2prouter. Simplemente ejecute “i2prouter start” en un terminal. (Nota: ¡no use sudo ni lo ejecute como root!)
- como un servicio que se ejecuta automáticamente cuando inicia su sistema, aún antes de loguearse. El servicio puede ser habilitado con “dpkg-reconfigure i2p” como root o mediante sudo. Esta es la manera recomendada.



# 50

## Bittorrent anónimos con I2PSnark

Podemos utilizar la red I2P para compartir y descargar archivos sin necesidad de que todo el mundo sepa que los está compartiendo, o que se está ejecutando un cliente de torrent, ya que la red I2P está cifrada de extremo a extremo y lo único que se ve desde afuera es que está corriendo I2P.

I2P viene con un cliente de torrent incorporado que se ejecuta dentro del navegador llamado I2PSnark. Puede acceder a través del siguiente enlace:

<http://localhost:7657/i2psnark/>

o a través de la consola del router: <http://localhost:7657/> haciendo click en el ícono del torrent. Una vez lanzado aparecerá una pantalla similar a la siguiente:

Puede buscar un torrent usando uno de los siguientes trackers de bittorrent:

- <http://tracker.postman.i2p/>
- <http://diftracker.i2p/>

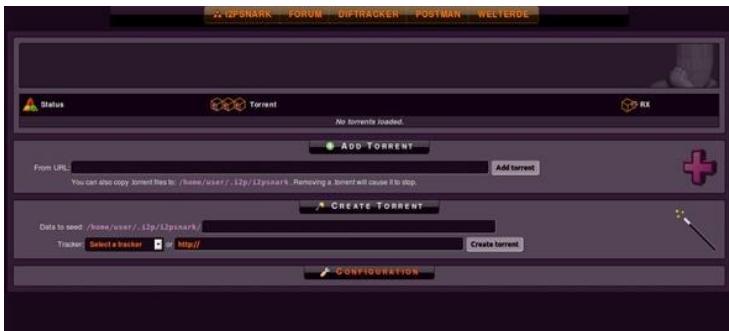


Figure 50.1: I2P

Copie el torrent o el enlace magnet y péguelo en la ventana de I2PSnark, luego haga click en **Add torrent**. El archivo se descargará en la carpeta **/home/user/.i2p/i2psnark**.

#### NOTA:

- Como I2P es una red cerrada, no se pueden descargar los torrents normales que se encuentran en Internet, ¡y no puede ser utilizada para hacer la descarga anónimamente!
- La velocidad parece ser un poco más baja de lo habitual debido a la anonimización. Las velocidades de descarga son aceptables si se tiene en cuenta que lo está haciendo de forma anónima. # OnionShare

## Introducción

¿Qué esOnionShare? Según las palabras de los propios dueños del proyecto (cita extraída de <https://github.com/micahflee/onionshare/blob/master/README.md>):

---

OnionShare le permite a usted compartir archivos de cualquier tamaño segura y anónimamente. Funciona mediante un servidor web, que es accesible mediante un servicio Tor oculto, y genera una URL imposible de adivinar para acceder y descargar los archivos. Esto no requiere que se configure un servidor en algún lugar de Internet o usar algún servicio de terceros para compartir servicios. Usted hospeda el archivo en su propia computadora y usa un servicio oculto de Tor para que esté temporalmente accesible en Internet. El resto de los usuarios solamente necesitan usar el navegador web de Tor para descargar su archivo.

## Instalación

Las instrucciones de instalación se encuentran en el sitio web de OnionShare.

## Como usar OnionShare

La siguiente es la pantalla de inicio de OnionShare.

Usted puede compartir tantos archivos y carpetas como quiera. Para añadirlas puede usar el botón correspondiente o arrastrar y soltar las carpetas dentro de la ventana. Por favor seleccione la opción **Stop sharing automatically**. Esto le asegura que los archivos que usted comparte puedan ser descargados solamente una vez.

Cliqueando el botón **Start Sharing** se lanza un pequeño servidor web en segundo plano. Esto le permite a su amigo descargar el archivo pero solamente a través de la red Tor porque dicho

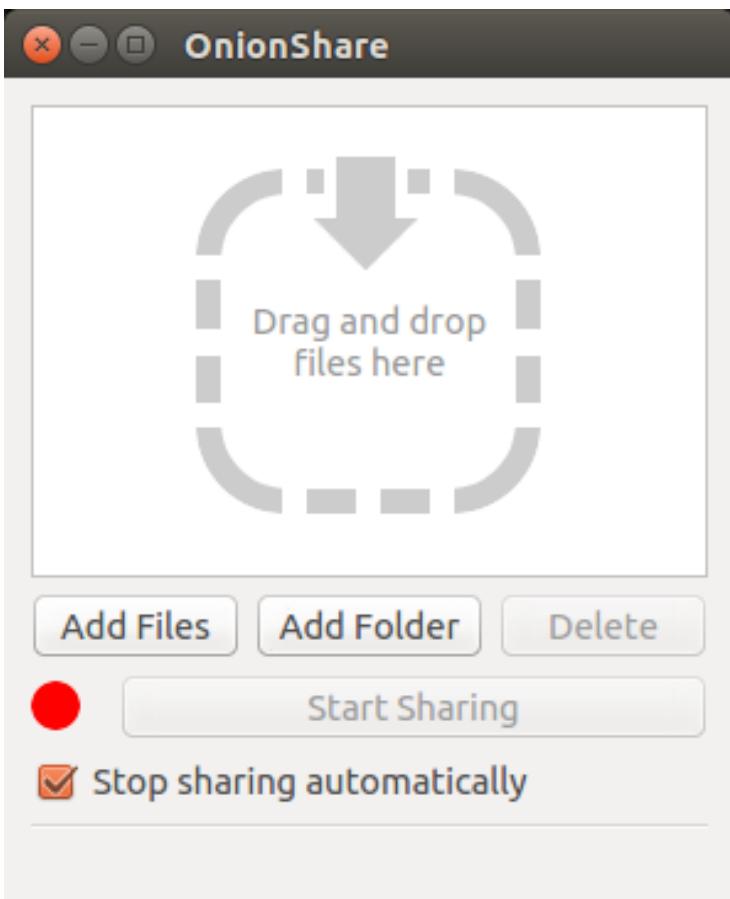


Figure 50.2: started OnionShare

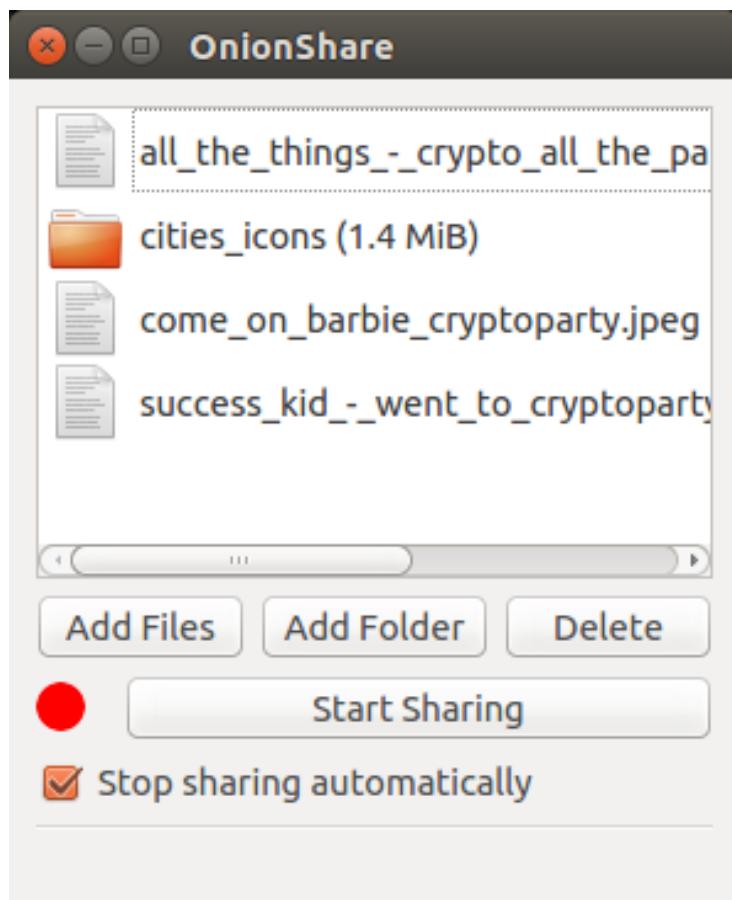


Figure 50.3: added files and folders

pequeño servidor es un servicio Tor oculto. El inicio del servicio oculto puede demorar un poco, por favor, sea paciente.

Una vez que el servicio oculto inicie, copie su url mediante el botón **Copy URL**. Luego, envíe dicha dirección a su amigo (si es necesario, a través de un canal cifrado).

Después de recibir la dirección su amigo debe abrirla en su navegador web Tor. Esta no será accesible desde otros navegadores web. Su amigo verá un enlace a un archivo comprimido en formato zip y una lista de archivos contenidos en su interior. La descarga se inicia cliqueando el gran botón azul.

Usted puede ver cuando su amigo descarga los archivos mediante la barra de progreso azul. Una vez que todo ha terminado, OnionShare detendrá el intercambio de archivos automáticamente (excepto que haya deseleccionado **Stop sharing automatically**).

Para verificar que OnionShare ha detenido efectivamente el intercambio de archivos puede abrir la dirección que le había enviado a su amigo en su propio navegador Tor. La descarga ya no está disponible.

0xcaca0 Adam Hyde Ahmed Mansour Alice Miller A Ravi Ariel Viera Asher Wolf AT Austin Martin Ben Weissmann Bernd Fix Brendan Howell Brian Newbold Carola Hesse Chris Pinchen Dan Hassan Daniel Kinsman Danja Vasiliev Dévai Nándor djmattyg007 Douwe Schmidt Edward Cherlin Elemar Emile Denichaud Emile den Tex Erik Stein Erinn Clark Freddy Martinez Freerk Ohling Greg Broiles Haneef Mubarak helen varley jamieson Janet Swisher Jan Gerber Jannette Mensch Jens Kubieziel jmorahan Josh Datko Joshua Datko Julian Oliver Kai Engert Karen Reilly l3lackEyedAngels leoJ3n LiamO Lonneke van der Velden Malte Malte Dik Marta Peirano Mart van Santen mdimitrova Michael Henriksen Nart Villeneuve Nathan Andrew Fain Nathan Houle Niels Elgaard Larsen

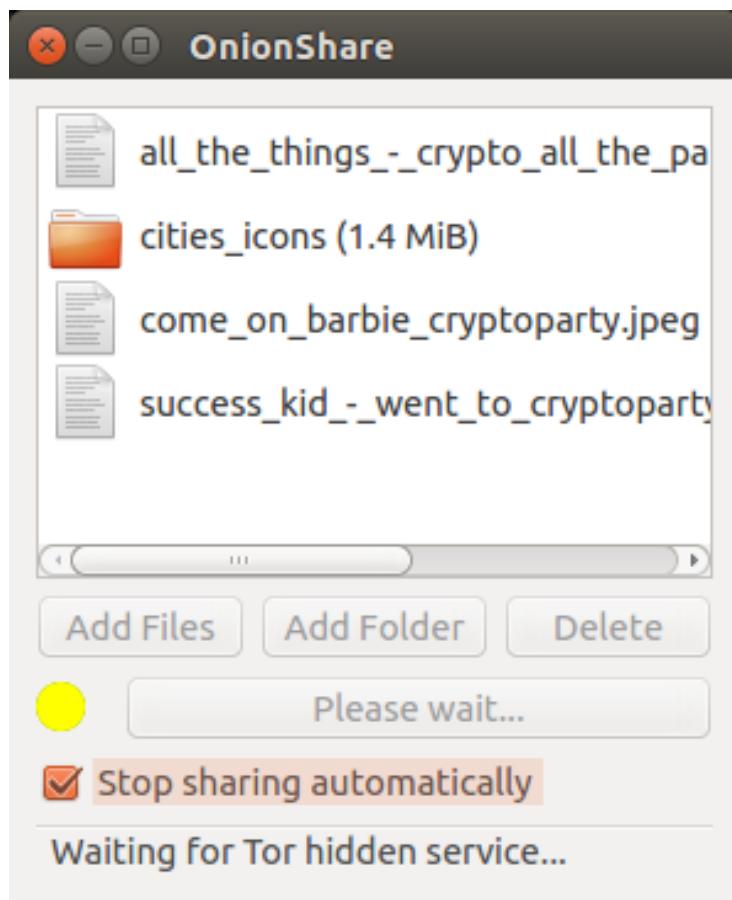


Figure 50.4: preparing to share files

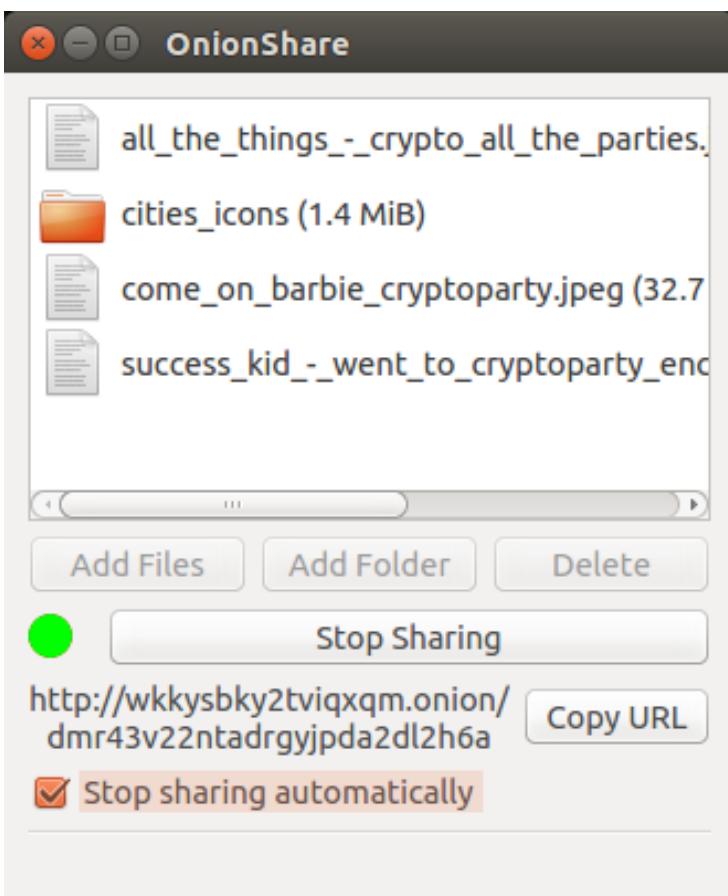


Figure 50.5: sharing files

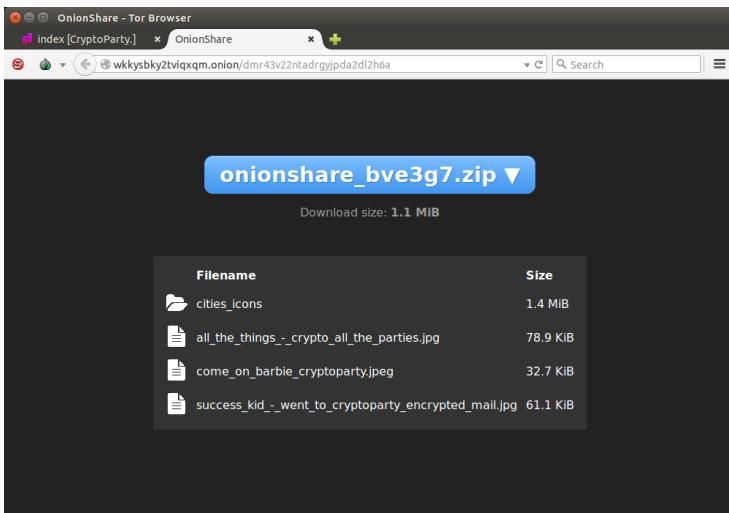


Figure 50.6: downloading through TorBrowser

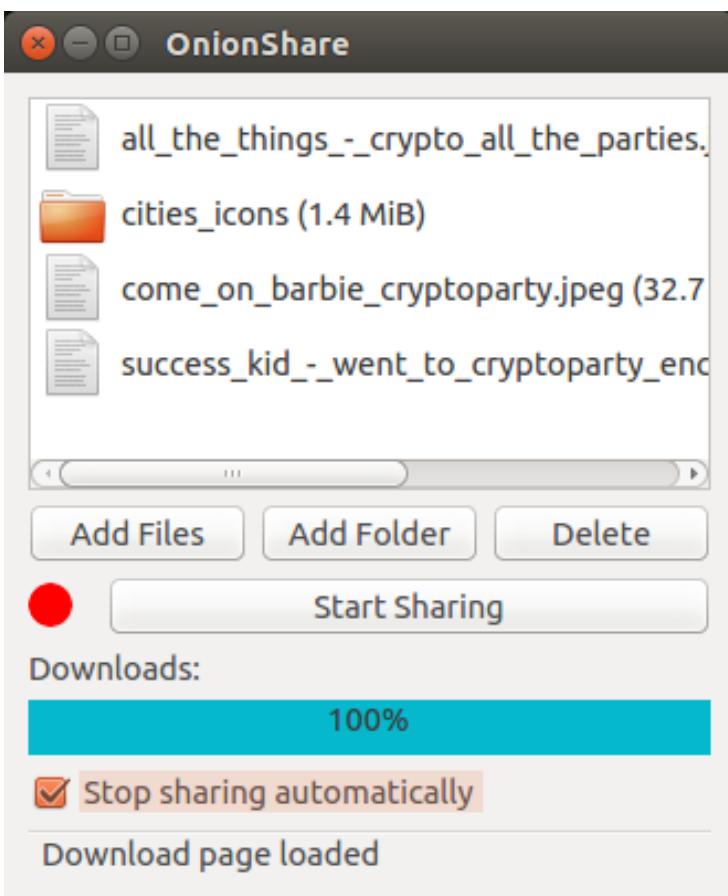


Figure 50.7: completed download as seen in OnionShare

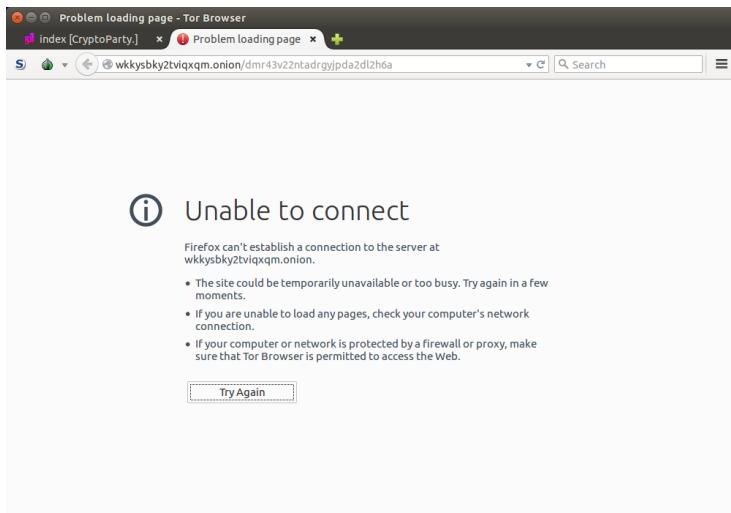


Figure 50.8: trying download through TorBrowser a second time

Petter Ericson Piers Plato Punkbob Roberto Rastapopoulos  
Ronald Deibert Ross Anderson Sacha van Geffen Sam Tennyson  
Samuel Carlisle Samuel L. Tennyson Seth Schoen Steven Murdoch  
StooJ Story89 Ted W Ted Wood Teresa Dillon therealplato  
Tomas Krag Tom Boyle Travis Tueffel Uwe Lippmann WillMorrison  
Ximin Luo Yuval Adam zandi Zorrino Zorrinno  
Criptografía y cifrado =====

Criptografía y cifrado son términos similares, el primero es la ciencia y el segundo la implementación. La historia del tema se remonta a las civilizaciones antiguas, cuando los primeros seres humanos comenzaron a organizarse en grupos. Esto se debió, en parte, al darse cuenta de que estábamos en competencia por los recursos y la organización tribal, conflictos y demás necesarios para mantenerse en la cima. En este sentido, la criptografía y el cifrado se basan en la guerra, la progresión y la gestión de recursos, en los que es necesario enviar mensajes secretos el uno al otro sin que el enemigo pueda descifrarlos.

La escritura es en realidad una de las primeras formas de cifrado que no todo el mundo puede leer. La palabra criptografía proviene de las palabras griegas kryptos (oculto) y graphein (escritura). En este sentido la criptografía y el cifrado en su forma más simple se refieren a la escritura de mensajes ocultos, que requieren un sistema o regla para descifrar y leer. Básicamente, esto le permite proteger su privacidad mediante la codificación de información de una manera que sólo es recuperable con cierto conocimiento (contraseñas o frases de paso) o posesión (una clave).

Dicho de otro modo, el cifrado es la traducción de la información escrita en texto plano en una forma no legible (texto cifrado) mediante esquemas algorítmicos (cifrados). El objetivo es utilizar la clave correcta para abrir el mensaje y regresarlo de nuevo a su forma original de texto plano para que sea legible.

Aunque la mayoría de los métodos de cifrado se refieren a la

---

palabra escrita, durante la Segunda Guerra Mundial, el ejército de EE.UU. utilizó indios Navajos, que viajaban entre los campamentos enviando mensajes en su lengua nativa. La razón por la que el ejército utilizó la tribu Navajo era proteger la información que se enviaba de las tropas japonesas, que no podían descifrar el idioma navajo hablado. Este es un ejemplo muy simple de usar un lenguaje para enviar mensajes que no queremos que la gente escuche o que sepa lo que estamos discutiendo. ¿Por qué es tan importante el cifrado?

Las redes informáticas y de telecomunicaciones almacenan los ecos digitales o huellas de nuestros pensamientos y los registros de nuestra vida personal.

Desde la banca, hasta las reservaciones, pasando por la socialización: nosotros enviamos una gran variedad de información detallada y personalizada, que está impulsando nuevos modelos de negocios, de interacción social y de conducta. Ahora nos hemos acostumbrado a dar lo que era (y sigue siendo) información considerada privada a cambio de lo que se presenta como un servicio más personalizado y a nuestra medida, que podría satisfacer nuestras necesidades, pero en realidad alimenta nuestra codicia.

Pero, ¿cómo protegemos de quienes nos observan, controlan y utilizan esta información?

Vamos a considerar un escenario en el que las cosas funcionan muy bien y podemos enviar toda nuestra comunicación en tarjetas postales abiertas escritas a mano. Desde las conversaciones con su médico, pasando por los momentos íntimos con sus amantes, hasta las discusiones legales que usted pueda tener con abogados o contadores. Es poco probable que nos guste que todas las personas sean capaces de leer dichas comunicaciones. Por esto, escribimos cartas en sobres cerrados, monitoreamos los envíos del correo, disponemos de oficinas cerradas y acuerdos confidenciales, que ayudan a mantener la comunicación privada.

Sin embargo, dado el cambio en la forma en que nos comunicamos, mucho más que este tipo de interacción se está llevando a cabo online. Más importante aún, se lleva a cabo a través de los espacios online, que no son privados de forma predeterminada y están abierta a personas con pocos conocimientos técnicos para husmear en los asuntos más importantes de nuestra vida.

La privacidad online y el cifrado es algo de lo que tiene que ser consciente y practicarlo todos los días. De la misma manera que pondría una carta importante en un sobre o tendría una conversación privada detrás de una puerta cerrada. Teniendo en cuenta que gran parte de nuestra comunicación privada está pasando ahora en los espacios en red y online, debemos considerar la interfaz, como los sobres o sellos que protegen este material como una necesidad básica y un derecho humano.

## Ejemplos de cifrado

A lo largo de la historia encontramos ejemplos de métodos de cifrado, que han sido usados para mantener a los mensajes privados y secretos.

## ¡Una advertencia!

“Existen dos clases de criptografía en el mundo: la que evitará que tu hermanita acceda a tus archivos, y la que detendrá a la mayoría de los gobiernos cuando quieran acceder a tus archivos” - Bruce Schneier, *Applied Cryptography*, 1996

Este capítulo primero explica un número de sistemas de cifrado históricos y luego proporciona un resumen de las técnicas más

---

modernas. Los ejemplos históricos ilustran como surgió la criptografía, pero se considera obsoleta desde la aparición de las computadoras modernas. Pueden ser divertidos para aprender, pero por favor no los use para nada realmente importante.

## Cifrado histórico

El cifrado clásico se refiere al cifrado histórico, que está fuera de uso o no es muy aplicable. Existen dos categorías generales de cifrado clásico: trasposición y sustitución.

En el cifrado por trasposición, las cartas mismas se mantienen sin cambios, pero el orden dentro del mensaje se codifica de acuerdo con un esquema bien definido. Un ejemplo de un cifrado de transposición es la escítala, que fue utilizada en la antigua Roma y Grecia. Se envolvía una cinta de papel alrededor de una vara y se escribía el mensaje a lo largo. De esta forma el mensaje no se podía leer a menos que la cinta se envolviese nuevamente alrededor de una vara del mismo diámetro.



Figure 50.9: Escítala

*Imagen: escítala, extraída de Wikimedia Commons (3.10.12)*

El cifrado por sustitución es una forma clásica de cifrado mediante el cual las letras o un grupo de ellas se reemplazan sistemáticamente a través del mensaje por otras letras (o un grupo

de ellas). El cifrado de sustitución se divide en monoalfabético y polialfabético. El cifrado por desplazamiento del César es un ejemplo común de cifrado por sustitución monoalfabética, donde las letras del abecedario son desplazadas en una sola dirección.

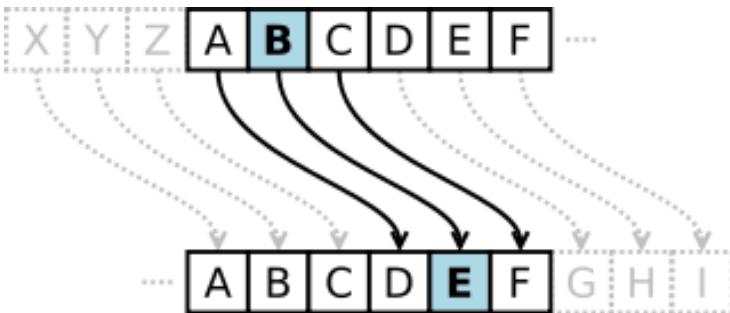


Figure 50.10: Cifrado del César

*Imagen: Cifrado por desplazamiento del César, extraída de Wikimedia Commons (3.10.12)*

Las sustituciones polialfabéticas son más complejas que el cifrado por sustitución porque usan más de un alfabeto y girado. Por ejemplo, el cifrado de Alberti, el primer cifrado polialfabético, fue creado en el siglo XV por León Battista Alberti, un erudito y humanista renacentista italiano al que también se lo conoce como el fundador de la criptografía occidental. Su cifrado es similar al cifrado de Vigenère, donde cada letra del alfabeto tiene un número único (por ejemplo, 1-26). El mensaje se cifra escribiendo la contraseña repetidamente por debajo de él.

En el cifrado Vigenère los números correspondientes a las letras del mensaje y la clave se suman (los números que exceden al alfabeto se redondean hacia abajo) haciendo que el mensaje

---

fuera tan difícil de leer que no podía ser descifrado por siglos (hoy en día, con la ayuda de las computadoras, esto obviamente no es cierto ya).

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	Y	

Figure 50.11: Cifrado de Vigenère

*Imagen: Cifrado de Vigenère, extraída de Wikimedia Commons (3.10.12)*

Durante la Segunda Guerra Mundial se produjo la explosión de la criptografía, que condujo al desarrollo de nuevos algoritmos, como la libreta de un solo uso (OTP). El algoritmo de OTP

combina texto plano con una clave aleatoria que es tan larga como el texto plano de forma que cada carácter sólo se utiliza una vez. Para utilizarlo se necesitan dos copias de la libreta, una para cada usuario y el intercambio a través de un canal seguro. Una vez que el mensaje se codifica con la libreta, ésta se destruye y el mensaje codificado es enviado. Del lado del receptor, se utiliza la libreta para descifrar el mensaje. Una manera de entender el algoritmo de OTP es pensar en él como una fuente de ruido del 100%, que se utiliza para emmascarar el mensaje. Dado que ambas partes de la comunicación tienen copias de la fuente de ruido son las únicas personas que pueden filtrarlo.

El algoritmo OTP se encuentra presente en varios sistemas de cifrado de flujo, que se explican a continuación. Claude Shannon, (un participante clave en la criptografía moderna y en la teoría de la información), en su artículo fundamental de 1949, “Teoría de la Comunicación de Sistemas Secretos” demuestra teóricamente que todo sistema de cifrado irrompibles debe incluir el cifrado OTP, el cual de ser usado correctamente es imposible de descifrar.

## Cifrado moderno

Tras las guerras mundiales del campo de la criptografía se alejó del servicio público y se redujo más al ámbito de los gobiernos. Los principales avances en el campo aparecieron en la década del 70 con el advenimiento de las computadoras personalizadas y la introducción del estándar de cifrado de datos (DES, desarrollado por IBM en 1977 y adoptada más tarde por el gobierno de los EE.UU.). Ahora, a partir del 2001, utilizamos la AES, (Advanced Encryption Standard), que se basa en formas de cifrado simétrico.

---

La criptografía moderna se puede dividir generalmente en tres partes: criptografía simétrica, asimétrica y cuántica.

La criptografía simétrica o de clave secreta, se refiere a sistemas de cifrado que utilizan la misma clave para cifrar y descifrar el texto o la información involucrada. En esta clase de sistemas de cifrado la clave se comparte y se mantiene en secreto dentro de un grupo restringido y por lo tanto no es posible ver la información cifrada sin tener la clave. Una simple analogía con la criptografía de clave secreta es el acceso restringido a un parque comunitario, donde existe llave para abrir la puerta, que es compartida por la comunidad. No puede abrir la puerta, a menos que tenga la llave. Obviamente, el problema aquí con la llave del jardín y con la clave del cifrado simétrico es si caen en las manos equivocadas, entonces un intruso o un atacante puede ingresar y la seguridad del jardín, o los datos y la información se verá comprometida. Por lo tanto uno de los principales problemas con este tipo de cifrado es el tema de la gestión de claves. Por lo dicho anteriormente, este método es más utilizado cuando existe un único usuario o en contextos o entornos de grupos pequeños.

A pesar de esta limitación los métodos de cifrado simétricos son considerablemente más rápido que los métodos asimétricos y también son el mecanismo preferido para cifrar grandes trozos de texto.

Los sistemas de cifrado simétricos suelen ser implementado usando **cifrados de bloque** \*\* o **cifrados de flujo**.

Los cifrados de bloque trabajan tomando los datos de entrada en bloques de 8, 16 o 32 bytes a la vez y mezclando los datos con la clave dentro de dichos bloques. Se realizan diferentes operaciones sobre los datos con el fin de transformarlos y mezclarlos dentro de los bloques. Tales sistemas de cifrado utilizan una clave secreta para convertir un bloque fijo de texto plano en texto cifrado. La misma clave se utiliza entonces para descifrar

el texto cifrado.

En comparación con el cifrado de flujo (también conocido como cifrado de estado), trabaja con cada dígito de texto plano mediante la creación de un flujo de clave correspondiente que forma el texto cifrado. El flujo de clave se refiere a una secuencia de caracteres aleatorios (bits, bytes, números o letras) en el que se llevan a cabo diversas sumas o restas combinadas sobre un carácter en el mensaje de texto plano, que produce entonces el texto cifrado. Aunque este método es muy seguro, no siempre es práctico, ya que la clave de la misma longitud que el mensaje tiene que ser transmitido de alguna manera segura de modo que el receptor puede descifrar el mensaje. Otra limitación es que la clave sólo puede ser utilizado una vez y después debe ser desecharada. Aunque esto puede significar mayor seguridad, limita el uso del cifrado.

Los sistemas de cifrado asimétricos trabajan con problemas matemáticos más complejos con puertas traseras, lo que permite soluciones más rápidas en las piezas de datos pequeñas muy importantes. También trabajan con tamaños de datos fijos, por lo general 1024-2048 bits y 384 bits. Lo que los hace especiales es que ayudan a resolver algunos de los problemas con la distribución de claves mediante la asignación de una par, una clave pública y otra privada por persona, así que todo el mundo sólo necesita saber todas las demás claves públicas. Los sistemas de cifrado asimétricos se usan también para firmas digitales. Los cifrados simétricos se utilizan generalmente para la autenticación del mensaje. Los sistemas de cifrado simétrico no pueden no repudiar firmas (es decir, las firmas que después usted no puede negar que firmó). Las firmas digitales son muy importantes en la criptografía moderna. Son similares a los sellos de cera con los cuales se verificaba de quién provenía el mensaje y al igual que ellos, son exclusivos de cada persona. Las firmas digitales son uno de los métodos utilizados en sistemas de clave pública, que han transformado

---

el campo de la criptografía y son esenciales para la seguridad en Internet y en las transacciones online.

## Criptografía cuántica

Criptografía cuántica es el término usado para describir el tipo de criptografía necesaria para tratar con la velocidad con la cual nosotros procesamos información y las medidas de seguridad relacionadas que son necesarias. Esencialmente consiste en usar comunicación cuántica para asegurar el intercambio de una clave y sus distribuciones asociadas. Como las máquinas que usamos se han vuelto más rápidas las posibles combinaciones de cifrado de clave pública y firmas digitales se han vuelto más vulnerables y la criptografía cuántica trata con los tipos de algoritmos que son necesarios para mantenerse al tanto con las redes más avanzadas.

## Desafíos e implicaciones

En el corazón de la criptografía está el reto de cómo usar y comunicar información. Los métodos anteriores describen cómo cifrar la comunicación escrita, pero, obviamente, como se muestra en el ejemplo Navajo, otros medios de comunicación (voz, sonido, imagen, etc) también se pueden cifrar utilizando diferentes métodos.

El objetivo principal y la habilidad del cifrado consiste en aplicar los métodos adecuados para brindar una comunicación confiable. Esto se logra mediante la comprensión de las ventajas y desventajas, fortalezas y debilidades de los diferentes métodos de cifrado y su relación con el nivel de seguridad y privacidad

necesarias. Obtener este derecho depende de la tarea y el contexto.

Es importante destacar que cuando hablamos de comunicación, estamos hablando acerca de la confianza. Tradicionalmente, la criptografía se ocupaba de los escenarios hipotéticos, donde el desafío era cómo hacer que ‘Bob’ pudiera hablar con ‘Alice’ de una manera privada y segura.

Nuestras vidas están ahora fuertemente entrelazadas con las computadoras e Internet. De modo que los límites entre Bob, Alice y el “otro” (Eva, Oscar, el Gran Hermano, su jefe, el ex-novio o el gobierno) son mucho más borrosos. Teniendo en cuenta el gran avance en el procesamiento de datos con computadoras, para ‘nosotros’, para que Bob y Alice puedan confiar en el sistema, tenemos que saber con quién están hablando demasiado, necesitamos saber quién está escuchando y lo más importante quién tiene el potencial para espionar . Lo que resulta importante es cómo navegar por esta complejidad y sentir que mantenemos el control y la seguridad, para poder participar y comunicarnos de una manera confiable, respetando nuestras libertades individuales y nuestra privacidad. Glosario =====

Gran parte de este contenido está basado en <http://en.cship.org/wiki/Special:Allpages>

## Administrador de contraseñas

Un administrador de contraseñas es software que ayuda al usuario para organizar sus contraseñas y códigos PIN. El software generalmente tiene una base de datos local o un archivo que mantiene los datos de las contraseñas cifrados para conectarse en forma segura con otras computadoras, redes, sitios web y archivos de aplicaciones. KeePass <http://keepass.info/> es un ejemplo.

---

## Agregador

Un agregador es un servicio que ofrece información recolectada de un sitio y lo pone disponible en diferentes direcciones. Se lo conoce también como agregador RSS, agregador de feeds, lector de feeds, o lector de noticias (No se debe confundir con el lector de noticias de Usenet)

## Análisis de amenazas

Un análisis de amenazas a la seguridad es un estudio formal, adecuado al detalle, de todas las maneras conocidas de ataques a la seguridad de los servidores o los protocolos, o de los métodos usados para un propósito particular tales como evasión. Las amenazas pueden ser de carácter técnico, como romper el código o explotar los errores de software, o sociales, como el robo de contraseñas o sobornar a alguien que tiene un conocimiento especial. Pocas compañías o individuos tienen el conocimiento y la habilidad para hacer un análisis global, pero todos los implicados tienen que hacer alguna estimación de los temas.

## Análisis de tráfico

El análisis de tráfico consiste en el análisis estadístico de las comunicaciones cifradas. En algunas circunstancias puede revelar información acerca de la gente comunicada y la información que están compartiendo.

## Ancho de banda

El ancho de banda de una conexión es la máxima velocidad de transferencia de datos, limitada por su capacidad y las características de las computadoras en ambos extremos de la conexión.

## Anonimato

(No se debe confundir con privacidad, seudoanonimato, seguridad o confidencialidad)

El anonimato en Internet es la capacidad de utilizar los servicios sin dejar pistas sobre su identidad o sin ser espiado. El nivel de protección depende de las técnicas de anonimato utilizados y el grado de seguimiento. Los más fuertes técnicas en uso para proteger el anonimato implican la creación de una cadena de comunicación a través de un proceso aleatorio para seleccionar algunos de los enlaces, en la que cada eslabón tiene acceso a la información parcial sobre el proceso. El primero conoce la dirección del usuario de Internet (IP), pero no el contenido, el destino o finalidad de la comunicación, ya que el contenido del mensaje e información de destino están cifrados. El último conoce la identidad del sitio que se está en contacto, pero no la fuente de la sesión. Algunos pasos intermedios entre los enlaces impiden que el primero y el último comparten su conocimiento parcial con el fin de conectar el usuario y el sitio de destino.

## Archivo de registro

Un archivo de registro es un archivo que guarda una secuencia de mensajes enviados por algún proceso de software, el cual

---

puede ser una aplicación o un componente del sistema operativo. Por ejemplo, los servidores web o los proxies pueden mantener registros que contienen información acerca de cuáles direcciones IP usan estos servicios y cuándo acceden y a qué páginas.

## **ASP (proveedor de servicios de aplicaciones)**

Un ASP es una organización que ofrece software sobre Internet, permitiendo actualizarlo y mantenerlo en forma centralizada.

## **Ataque por fuerza bruta**

Un ataque por fuerza bruta consiste en tratar de averiguar una contraseña probando todos las variantes posibles. Es uno de los ataques de hacking más básicos.

## **Backbone**

Un backbone (a veces llamado red troncal) es uno de los enlaces de comunicaciones de gran ancho de banda que une redes en diferentes países y organizaciones alrededor del mundo en Internet.

## **Badware**

Consulte *malware*.

## Bash (Bourne-again shell)

El shell bash es una interfaz de línea de comandos para sistemas operativos GNU/Linux o Unix, basado en el shell Bourne.

## BitTorrent

BitTorrent es un protocolo para compartir archivos entre pares, inventado por Bram Cohen en 2001. Permite a los individuos distribuir de forma barata y eficaz archivos de gran tamaño, como imágenes de CD, video o archivos de música.

## Bluebar

La barra azul de URL (llamada en la jerga Bluebar Psiphon) es la forma en la parte superior de la ventana del navegador del nodo Psiphon que le permite acceder al sitio bloqueado escribiendo su URL en el interior.

Vea también *nodo Psiphon*.

## Bloqueo

El bloqueo impide el acceso a un recurso de Internet, basado en un gran número de métodos.

---

## Caché

La caché es una parte de un sistema de procesamiento de información usada para almacenar datos usados en forma reciente o muy frecuente con el fin de acelerar el acceso repetido a ellos. Una caché web mantiene copias de los archivos de la página web.

## Censorware

Censorware es software usado para filtrar o bloquear el acceso a Internet. Este término se usa a menudo para referirse al software instalado en la máquina cliente (la computadora usada para acceder a Internet). La mayoría del censorware se utiliza con propósitos de control parental. Algunas veces el término censorware se utiliza también para referirse al software usado con los mismos propósitos pero instalado en un servidor de red o un router.

## Censura

Censurar es evitar la publicación o recuperación de información, o tomar medidas, legales o de otro tipo, contra los editores y lectores.

## CGI (Interfaz de gateway común)

CGI es un estándar de uso común que permite a los programas de un servidor web ejecutarse como aplicaciones. Algunas páginas web basadas en proxy usan CGI, por lo que se denominan

“proxies CGI”. (Una de las más populares aplicaciones escrita por James Marshall usa el lenguaje de programación Perl y se denomina CGIPProxy.)

## Cifrado

Se denomina así a todo método usado para recodificar y mezclar datos o transformarlos matemáticamente para que sea ilegible a las terceras partes y por lo tanto, no puedan descifrar el secreto que oculta. Es posible cifrar datos en su disco rígido local usando software como TrueCrypt (<http://www.truecrypt.org>) o cifrar el tráfico de Internet con TLS/SSL o SSH.

vea también *descifrado*.

## Cifrado completo de disco

vea *cifrado de disco*.

## Cifrado de disco

El cifrado de disco es una tecnología que protege la información al convertirla en ilegible para que no pueda ser descifrada fácilmente por personas no autorizadas. Usa software o hardware para cifrar cada bit de datos que está en un disco o en un volumen de disco. El cifrado de disco previene el acceso no autorizado a los datos almacenados.

---

## Clave pública

vea *criptografía de clave pública/cifrado de clave pública*.

## Código (de cifrado)

En criptografía, un código es un algoritmo para realizar cifrado o descifrado de mensajes.

## Confidencialidad directa perfecta (PFS)

En un protocolo de acuerdo de claves autenticadas que utiliza la criptografía de clave pública, la confidencialidad directa perfecta (PFS) o es la propiedad que asegura que una clave de sesión derivada de un conjunto de claves públicas y privadas de largo plazo no se verá comprometida si una de las claves privadas (a largo plazo) se ve comprometida en el futuro.

## Cookie

Un cookie es una cadena de texto enviado por un servidor web al navegador del usuario para almacenarla en su computadora, conteniendo información necesaria para mantener la continuidad en las sesiones a través de múltiples páginas web, o a través de múltiple sesiones. Algunos sitios web no se pueden usar sin aceptar ni almacenar una cookie. Algunas personas consideran esto como una invasión a la privacidad y/o un riesgo de seguridad.

## Criptografía

La criptografía es la práctica y el estudio de las técnicas para establecer comunicaciones seguras en presencia de terceras partes (los llamados adversarios). En forma más general, consiste en la construcción y análisis de protocolos para vencer a nuestros adversarios en varios aspectos relacionados con la seguridad de la información tales como confidencialidad, integridad, autenticación y no repudio de datos. La criptografía moderna abarca un amplio rango de disciplinas tales como matemáticas, ciencias de la computación e ingeniería eléctrica. Sus aplicaciones incluyen tarjetas ATM, contraseñas de computadoras y comercio electrónico.

## Criptografía de clave pública/cifrado de clave pública

La criptografía de clave pública se refiere al sistema de cifrado que requiere dos claves separadas, una de las cuales es secreta y la otra pública. Aunque son diferentes, ambas claves están relacionadas matemáticamente. Una clave cifra el texto plano y la otra lo descifra. Ninguna clave puede realizar ambas funciones. Una de ellas puede ser publicada, mientras que la otra debe mantenerse en privado.

La criptografía de clave pública usa algoritmos de clave asimétricos (tales como RSA), y se suele llamar por el término más general *criptografía de clave asimétrica*.

## Clave privada

vea *criptografía de clave pública/cifrado de clave pública*.

---

## **Chat**

El chat, también llamado mensajería instantánea, es un método habitual de comunicación entre dos o más personas en la cual cada línea tipeada por un participante en una sesión es vista por los otros. Existen numerosos protocolos, incluyendo aquellos creados por empresas específicas (AOL, Yahoo!, Microsoft, Google, y otros) y los definidos públicamente. Algunos clientes soportan un único protocolo, pero la mayoría utiliza una variedad de los protocolos más populares.

## **DARPA**

DARPA (Defense Advanced Projects Research Agency, Agencia de investigación de proyectos avanzados de defensa) es el sucesor de ARPA, que fundó Internet y su predecesor, ARPAnet.

## **Descifrado**

Descifrar es recuperar el texto plano u otros mensajes a partir de un mensaje cifrado mediante el uso de una clave.

Consulte también *cifrado*.

## **Dirección IP (dirección del protocolo de Internet)**

Una dirección IP es un número que identifica una computadora en particular en Internet. En la versión 4 (IPv4) consiste en cuatro bytes (32 bits), a menudo representada por cuatro

números enteros del rango de 0 a 255 separados por puntos, tal como 74.54.30.85. En IPv6, versión a la cual actualmente está cambiando la red, una dirección IP es cuatro veces más larga, y consiste de 128 bits. Puede ser escrita en 8 grupos de 4 dígitos hexadecimales separados por dos puntos, por ejemplo 2001:0db8:85a3:0000:0000:8a2e:0370:7334.

## Dirección IP públicamente ruteable

Las direcciones IP públicamente ruteables (a veces llamadas direcciones IP públicas) son aquellas que pueden alcanzarse de forma normal en Internet, a través de una cadena de enruteadores. Algunas direcciones IP son privadas, como el bloque 192.168.x.x, y muchas no están asignadas.

## DNS (Sistema de nombres de dominio)

El sistema de nombres de dominio (DNS) convierte los nombres de dominio, compuestos por combinaciones de letras fáciles de recordar, a las direcciones IP, que son cadenas de números difíciles de recordar. Cada computadora en Internet tiene una dirección única (algo parecido a un código de área + número telefónico)

## Dominio

Un dominio puede ser un dominio de nivel superior (TLD) o un dominio secundario de Internet.

Vea también *dominio de nivel superior*, *dominio de nivel superior con código país* y *dominio secundario*.

---

## **Dominio de alto nivel con código de país (ccTLD)**

Cada país tiene un código de dos letras, y un TLD (dominio de alto nivel) basado en él, tal como .ca para Canada; este dominio se llama dominio de alto nivel con código de país. Cada ccTLD tiene un servidor DNS que lista todos los dominios de segundo nivel dentro del TLD. Los servidores raíz apuntan a todos los TLD, y almacenan la información usada frecuentemente en los dominios de nivel inferior.

## **Dominio de nivel superior (TLD)**

En el ámbito de los nombres de Internet, el TLD es el último componente del nombre de dominio. Existen diversos TLD genéricos, los más importantes son .com, .org, .edu, .net, .gov, .mil, .int, y un código de país de dos letras (ccTLD) diferente para cada uno de ellos, por ejemplo, .ca for Canada. La Unión Europea también tiene código propio, .eu.

## **E-mail (correo electrónico)**

E-mail, abreviatura en inglés de correo electrónico, es un método para enviar y recibir mensajes por Internet. Se puede usar un servicio de web mail o enviarlos con el protocolo SMTP y recibirlas con el protocolo POP3 mediante un cliente de correo electrónico tal como Outlook Express o Thunderbird. Es raro que un gobierno bloquee el correo electrónico, sin embargo, la vigilancia es muy común. Si el correo electrónico no está cifrado, será muy fácil de leer por algún operador de red o un gobierno.

## Escuchas ilegales

Las escuchas ilegales consisten en interceptar al tráfico de voz o la lectura o filtrar el tráfico de datos en una línea telefónica o una conexión de datos digitales, por lo general para detectar o prevenir actividades ilegales o no deseadas o para controlar o monitorear lo que la gente está hablando.

## Esquema

En la Web, un esquema es una asignación de un nombre a un protocolo. Así, el esquema HTTP asigna URLs que comienzan con HTTP: el Protocolo de Transferencia de Hipertexto. El protocolo determina la interpretación del resto de la URL, por lo que `http://www.example.com/dir/content.html` identifica un sitio web y un archivo específico en un directorio específico, y `mailto: user@somewhere.com` es una dirección de correo electrónico de una persona o grupo específico en un dominio específico.

## Esteganografía

Esta palabra, que en griego significa escritura ocultar, se refiere a la variedad de métodos para enviar mensajes ocultos donde no sólo lo está el contenido, sino que también es muy probable que algo que lo encubra también lo esté. Generalmente se oculta una cosa dentro de otra, como una fotografía o un texto dentro de algo sin relación alguna. Contrariamente a la criptografía, donde está claro que se está transmitiendo un mensaje secreto, la esteganografía intenta ocultar también a la comunicación en sí misma.

---

## Evasión

La evasión es publicar o dar acceso a los contenidos, a pesar de los intentos de censura.

## Expresión regular

Una expresión regular (también conocida como regexp o RE) es un patrón de texto que especifica un conjunto de cadena de textos en una implementación particular de una expresión regular tal como la utilidad grep de UNIX. Una cadena de texto “encuentra” una expresión regular si la cadena concuerda con el patrón, como está definido en la sintaxis de la expresión regular. En cada sintaxis de RE, algunos caracteres tienen significados especiales, para permitir que un patrón encuentre múltiples cadenas. Por ejemplo, la expresión regular lo+se encuentra loose, loose, and looose.

## Filtro

Es alguna forma de búsqueda de patrones de datos para bloquear o permitir las comunicaciones.

## Filtro de bajo ancho de banda

Un filtro de bajo ancho de banda es un servicio web que remueve elementos extraños tales como publicidades e imágenes de una página web y además la comprime, haciendo mucho más rápida la descarga.

## Filtro de palabra clave

Un filtro de palabra clave escanea todo el tráfico de Internet que pasa a través de un servidor para hallar palabras o términos prohibidos para poder bloquearlas.

## Firefox

Firefox es el navegador web open source más popular, desarrollado por la Fundación Mozilla.

## Foro

En un sitio web, un foro es un lugar para la discusión, donde los usuarios pueden publicar mensajes y comentar otros previamente publicados. Se diferencia de una lista de correo o un grupo de Usenet por la persistencia de las páginas que contienen los hilos de los mensajes. Los archivos de grupo de noticias y listas de correo, sin embargo, muestran habitualmente un mensaje por página, con páginas de navegación que listan solamente las cabeceras de los mensajes en un hilo.

## Frame (marco)

Un frame es una porción de una página web que posee su propia URL. Por ejemplo, los frames se usan habitualmente para colocar un menú estático cercano a una ventana con texto deslizante.

---

## **FTP (Protocolo de transferencia de archivo)**

El protocolo FTP se usa para transferir archivos. Mucha gente lo usa generalmente para descargas; aunque se puede usar también para cargar páginas web y scripts para algunos servidores web. Usa habitualmente los puertos 20 y 21, que a veces están bloqueados. Algunos servidores FTP escuchan en otros puertos, pudiendo evadir el bloqueo basado en puertos.

Un cliente FTP popular libre para Windows y Mac OS es FileZilla. Existen también algunos clientes FTP basados en la web que pueden usarse con un navegador normal tal como Firefox.

## **Fuga de DNS**

Una fuga de DNS ocurre cuando un equipo que está configurado para usar un proxy para su conexión a Internet, sin embargo hace consultas DNS sin usarlo, lo que expone a los intentos de los usuarios para conectarse con sitios bloqueados. Algunos navegadores web tienen opciones de configuración para forzar el uso del proxy.

## **Gateway**

Un gateway es un nodo que conecta dos redes en Internet. Un ejemplo importante son los gateways nacionales a través de los cuales pasa todo el tráfico, tanto entrante como saliente.

## GNU Privacy Guard

GNU Privacy Guard (GnuPG o GPG) es una aplicación de software de criptografía, alternativa de PGP, con licencia libre GPL. Cumple con la especificación RFC 4880, la especificación estándar actual IETF de OpenPGP.

vea también *PGP*.

## PGP

vea *GNU Privacy Guard*.

## Honeypot

Un honeypot es un sitio web que simula ofrecer un servicio para tentar a usuarios potenciales para que lo usen, y poder capturar información sobre ellos o sus actividades.

## HTTP (Protocolo de transferencia de hipertexto)

HTTP es el protocolo fundamental de la World Wide Web, que proporciona métodos para solicitar y mostrar páginas Web, consultar y generar respuestas a las consultas, y el acceso a una amplia gama de servicios.

---

## **HTTPS (HTTP seguro)**

Es un protocolo de comunicación segura mediante cifrado de mensajes HTTP. Los mensajes entre el cliente y el servidor se cifran en ambas direcciones, utilizando claves generadas cuando la conexión se solicitó y se intercambiaron con seguridad. Las direcciones IP de origen y destino están en las cabeceras de cada paquete, así que HTTPS no puede ocultar el hecho de la comunicación, sólo el contenido de los datos transmitidos y recibidos.

## **IANA**

IANA (Internet Assigned Numbers Authority, autoridad de asignación de números de internet) es la organización responsable de los trabajos técnicos en la gestión de la infraestructura de Internet, incluyendo la asignación de bloques de direcciones IP para dominios de nivel superior y los registradores de licencias de dominio para los ccTLD y de los dominios de nivel superior genéricos, la ejecución de los servidores raíz de Internet, y otros funciones.

## **ICANN**

ICANN (Internet Corporation for Assigned Names and Numbers, corporación de internet para nombres y números asignados) es una corporación creada por el Departamento de Comercio de los EEUU para administrar los niveles más altos de Internet. El trabajo técnico lo lleva a cabo IANA.

## Mensajería instantánea (IM)

La mensajería instantánea se refiere a chatear usando protocolos propietarios, o a chatear en general. Los clientes de mensajería instantánea más comunes son MSN Messenger, ICQ, AIM o Yahoo! Messenger.

## Intermediario

vea *man in the middle*.

## Intercambio de archivos

El intercambio de archivos se refiere a cualquier sistema de computadora donde mucha gente puede usar la misma información, pero a menudo se refiere a música, películas u otros materiales disponibles libres de cargo en Internet.

## Interfaz común de gateway

vea *CGI*.

## Interfaz de línea de comandos

Es un método para controlar la ejecución de software usando comandos ingresados con un teclado, tal como un shell de Unix o una línea de comandos de Windows.

---

## **Internet**

Internet es una red de redes interconectadas que usan TCP/IP y otros protocolos de comunicación.

## **IRC (Internet relay chat)**

IRC es un protocolo de Internet de más de 20 años de antigüedad usado para conversaciones de texto en tiempo real (chat o mensajería instantánea). Existen distintas redes IRC, la mayor posee más de 50.000 usuarios.

## **ISP (Proveedor de servicio de internet)**

Un ISP (proveedor de servicio de Internet) es una empresa u organización que suministra acceso a Internet para sus clientes.

## **JavaScript**

JavaScript es un lenguaje de scripting, de uso habitual en las páginas web que suministran funciones interactivas.

## **KeePass, KeePassX**

KeePass y KeePassX son dos tipos de administradores de contraseñas.

## Latencia

La latencia es una medida del tiempo de demora experimentado en un sistema, en este contexto, en una computadora en la red. Se mide como el tiempo transcurrido entre el comienzo de la transmisión de un paquete y el comienzo de su recepción, entre un extremo de la red (por ejemplo usted) y el otro (por ejemplo el servidor web). Una manera muy poderosa de filtrado web es mantener una muy alta latencia, la que provoca que el uso de muchas herramientas de evasión sea muy dificultoso.

## Lista blanca

Una lista blanca (whitelist) es una lista de sitios específicamente autorizados para establecer alguna forma particular de comunicación. Se puede filtrar el tráfico con una lista blanca (bloqueando todo excepto los sitios de la lista), una lista negra (permitiendo todo excepto los sitios de la lista), una combinación de ambas u otras políticas basadas en reglas y condiciones específicas.

## Lista negra

Una lista negra (blacklist) es una lista de cosas prohibidas. Para la censura en Internet, es una lista de los sitios web o las direcciones IP de las computadoras prohibidas; se permite acceder a todos los sitios y/o computadoras excepto a aquellos listados específicamente. Una alternativa es una lista blanca, o lista de cosas permitidas. Una lista blanca bloquea el acceso a todos los sitios excepto a aquellos específicamente listados. No es muy común. Es posible combinar ambos tipos de listas usando cade-

---

nas de búsqueda u otras técnicas condicionales en URL que no coincidan con ninguna de las listas.

## Malware

Malware es un término general para referirse a software malicioso, incluyendo a los virus, que pueden estar instalados o pueden ser ejecutados sin su conocimiento. El malware toma el control de su computadora para fines específicos como, por ejemplo, enviar spam. (También se conoce al malware como badware.)

## Man in the middle

Un man in the middle (*hombre en el medio*) es una persona o computadora que captura tráfico en un canal de comunicación, principalmente para realizar cambios selectivos o bloquear el contenido de una manera que socave la seguridad criptográfica. En general, el ataque man-in-the-middle implica pasar por un sitio Web, servicio o individuo con el fin de registrar o alterar las comunicaciones. Los gobiernos pueden ejecutar man-in-the-middle en los gateways de entrada a un país por donde pasa todo el tráfico.

## Marcador

Un marcador es una referencia a una posición dentro del software que apunta a un recurso externo. En un navegador, es una referencia a una página web – al elegir un marcador usted

puede cargar rápidamente el sitio web sin necesidad de tipar la URL completa.

## Monitoreo

El monitoreo consiste en el control continuo de un flujo de datos en busca de actividad no deseada.

## Motor de difusión de archivos

Un motor de difusión de archivos es un sitio web editor que puede ser usado para eludir la censura. Un usuario sólo tiene que cargar el archivo a publicar una vez y el motor lo propaga a un conjunto de servicios de almacenamiento compartido (como Rapidshare o Megaupload).

## NAT (Traducción de dirección de red)

NAT es una función de un router para ocultar un espacio de direcciones de reasignación. Todo el tráfico que sale del router, utiliza su dirección IP, y el router sabe cómo enrutar el tráfico entrante a quien se lo solicite. NAT es frecuentemente aplicado por los cortafuegos. Puesto que las conexiones entrantes son normalmente prohibidas por NAT, se hace difícil ofrecer un servicio al público en general, como un sitio Web o un proxy público. En una red donde NAT está en uso, ofrecer este servicio requiere algún tipo de configuración de cortafuegos o método NAT transversal.

---

## Nodo

Un nodo es un dispositivo activo en una red. Un router es un ejemplo de un nodo. En las redes Psiphon y Tor, un servidor se conoce también como nodo.

## Nodo abierto

Un nodo abierto es un nodo específico Psiphon que puede ser usado sin loguearse. Éste carga automáticamente una página de inicio propia, y se presenta a sí mismo en un lenguaje propio, pero puede ser usado por cualquier navegador web.

vea también *nodo Psiphon*.

## Nodo de enlace o intermedio

Un nodo intermedio es un nodo Tor que no es un nodo de salida. La ejecución de un nodo intermedio puede ser más segura que la ejecución de un nodo de salida, porque un nodo intermedio no se mostrará en los archivos de registro de terceros. (Un nodo intermediario a veces se llama un nodo sin salida.)

## Nodo de salida

Un nodo de salida es un nodo Tor que reenvía datos fuera de la red Tor.

## Nodo privado

Un nodo privado es un nodo Psiphon que trabaja con autenticación, lo que significa que usted debe registrarse antes de poder usarlo. Hecho esto, podrá enviar invitaciones a su amigos para que usen este nodo específico. Vea también *nodo Psiphon*.

## Nodo Psiphon

Un nodo Psiphon es un proxy web seguro diseñado para evadir la censura en Internet. Fue desarrollado por Psiphon inc. Psiphon puede ser de código libre o privativo.

## Nodo sin salida

vea *nodo de enlace o intermedio*.

## Ofuscación

La ofuscación consiste en ocultar texto utilizando técnicas de transformación fáciles de entender y de revertir que resistan la inspección casual, pero no al criptoanálisis, o hacer cambios menores en las cadenas de texto para prevenir comparaciones simples. Los proxies Web suelen utilizar la ofuscación para ocultar ciertos nombres y direcciones de los filtros de texto simples que pueden ser engañados. Por ejemplo, cualquier nombre de dominio puede contener opcionalmente un punto final, como en “somewhere.com.”, Pero algunos filtros pueden buscar sólo “somewhere.com” (sin el punto final).

---

## **Operador de red**

Un operador de red es una persona u organización que mantiene o controla una red y se encuentra en posición de monitorear, bloquear o alterar la comunicación que pasa a través de su red.

## **OTR (mensajes sin registro)**

Un mensaje sin registro, comúnmente denominado OTR, es un protocolo criptográfico que suministra un cifrado fuerte para conversaciones de mensajería instantánea.

## **Paquete**

Un paquete es una estructura de datos definida por un protocolo de comunicación que contiene información específica en formas predeterminadas junto con datos arbitrarios para ser comunicados de un punto a otro. Los mensajes se dividen en partes que se almacenan en paquetes para ser transmitidos y luego se ensamblan en el otro extremo del enlace.

## **Pastebin**

Es un servicio web donde cualquier tipo de texto puede ser cargado y leído sin tener que registrarse. Todos los textos son visibles públicamente.

## P2P

Una red de pares (o P2P, *peer to peer*) es una red de computadoras entre iguales. A diferencia de las redes cliente-servidor no hay un servidor central por lo que el tráfico se distribuye sólo entre clientes. Esta tecnología se aplica sobre todo en los programas de intercambio como BitTorrent, eMule y Gnutella. Pero también la tecnología del muy antiguo Usenet o del programa de VoIP Skype VoIP se pueden clasificar como sistemas P2P.

vea también *compartir archivos*.

## PGP (Pretty Good Privacidad, *privacidad bastante buena*)

PGP es un programa de computadora para cifrado que suministra privacidad criptográfica y autenticación para comunicación de datos. Se utiliza a menudo para firmar, cifrar y descifrar textos, correos electrónicos, archivos, directorios y particiones de discos para incrementar la seguridad de las comunicaciones por correo electrónico.

PGP y otros productos similares siguen el estándar OpenPGP (RFC 4880) para cifrado y descifrado de datos.

## PHP

PHP es un lenguaje de scripting diseñado para crear sitios web dinámicos y aplicaciones web. Se instala en un servidor. Por ejemplo, el popular proxy web PHPProxy usa esta tecnología.

---

## **POP3**

El protocolo POP3 (Post Office Protocol version 3) es usado para recibir correos electrónicos de un servidor, por defecto en el puerto 110 con un programa de correo electrónico tal como Outlook Express o Thunderbird.

## **Privacidad**

La protección de la intimidad consiste en impedir la divulgación de información privada personal sin el consentimiento de la persona interesada. En este contexto, significa impedir que algunos observadores se enteren de que una persona haya solicitado o recibido información que ha sido bloqueada o es ilegal en el país donde se encuentre la persona en cuestión.

## **Protocolo**

Una definición formal de un método de comunicación, y la forma en que los datos deben ser transmitidos. Además, se refiere al propósito de tal método de comunicación. Por ejemplo, el protocolo para la transmisión de paquetes de datos en Internet (IP), o el protocolo de transferencia de hipertexto para las interacciones en la World Wide Web (HTTP).

## **Proxy Web**

Un proxy web es un script que se ejecuta en un servidor que actúa como un proxy/gateway. Los usuarios pueden acceder al proxy web con su navegador habitual (por ejemplo Firefox) e

ingresar cualquier URL en el formulario localizado en el sitio web. luego el programa del servidor recibirá el contenido y lo mostrará al usuario. De esta forma el ISP sólo verá una conexión al servidor con el proxy web ya que no se ha establecido una conexión directa.

## Puente

Vea *Puente Tor*

## Puente Tor

Un puente es un nodo intermedio que no está listado en el directorio público principal de Tor, por lo que es especialmente útil en países donde las comunicaciones están bloqueadas. A diferencia del caso de los nodos de salida, las direcciones IP de los nodos puente nunca aparecen en los archivos de registro del servidor y nunca pasan a través de los nodos de control de manera que pueden ser conectados con la evasión.

## Puerto

Un puerto de hardware en una computadora es un conector físico para un propósito específico que usa un protocolo de hardware propio. Algunos ejemplos son el puerto de la pantalla VGA o un conector USB.

Los puertos de software también conectan computadoras y otros dispositivos en las redes usando distintos protocolos, pero existen en el software solamente como números. Los puertos son

---

algo así como los números puestos sobre las puertas que dan acceso a distintas habitaciones, cada uno con un servicio especial en un servidor o en una PC. Están identificados por números enteros entre 0 y 65535.

## **Remailer**

Un remailer anónimo es un servicio que le permite a los usuarios enviar correos electrónicos anónimamente. El remailer recibe los mensajes y lo reenvía a su destinatario después de remover la información que podría identificar al remitente original. Algunos servicios también proveen una dirección anónima que puede ser usada para recibir las respuestas sin descubrir su identidad. Algunos servicios de remailer conocidos incluyen a Cypherpunk, Mixmaster y Nym.

## **Router**

Un router es una computadora que determina la ruta para reenviar paquetes. Utiliza la información de la dirección en la cabecera del paquete y la información de la caché en el servidor para hallar los números de dirección con conexiones de hardware.

## **RSS (agregador de noticias)**

RSS es un método y un protocolo que le permite a los usuarios de Internet suscribirse al contenido de una página web, y recibir actualizaciones tan pronto como sean publicadas.

## **Salto (Hope)**

Es un enlace en una cadena de paquetes transferidos desde una computadora a otra, o alguna computadora a lo largo de la ruta. El número de saltos entre computadoras puede brindar una estimación de la demora (latencia) en las comunicaciones entre ellas. Cada salto individual es también una entidad que posee la capacidad de escuchar, bloquear o alterar las comunicaciones.

## **Screenlogger**

Un screenlogger es un software capaz de registrar todo lo que su computadora muestra en la pantalla. Su principal característica es capturar la pantalla y el login en archivos para consultarlos en otro momento. Los screenloggers pueden utilizarse como una poderosa herramienta de monitoreo. Debe ser precavido con todas las pantallas de login que se ejecuten en la computadora que esté usando, en todo momento.

## **Script**

Un script es un programa, generalmente escrito en un lenguaje interpretado, no compilado (tal como JavaScript o Java), o en un lenguaje interpretado de comandos tal como bash. Muchas páginas web incluyen scripts para administrar la interacción con ella, y entonces el servidor no necesita reenviar cada página ante un nuevo cambio.

---

## **Script embebido**

Un script embebido es una pieza de código de software.

## **Servidor de nombre raíz**

Un servidor de nombre raíz es uno de los trece grupos de servidores administrados por la IANA para dirigir el tráfico a todos los dominios de primer nivel, como el núcleo del sistema DNS.

## **Servidor DNS**

A servidor DNS, o servidor de nombres, es un servidor que proporciona la función de consulta del sistema de nombres de dominio. Esto se hace ya sea mediante el acceso a un registro existente en caché de la dirección IP de un dominio específico, o mediante el envío de una solicitud de información a otro servidor de nombres.

## **Servidor proxy**

Un servidor proxy es un servidor, sistema de computadora o un programa de aplicación que funciona como pasarela entre un cliente y un servidor web. Un cliente se conecta al servidor proxy y envía una petición a una página web desde un servidor diferente. Luego el servidor proxy accede al recurso conectándose al servidor especificado, y devuelve la información al sitio solicitante. Los servidores proxy pueden servir para diferentes propósitos, incluyendo el acceso a páginas web prohibidas o para ayudar a los usuarios a enrutarse sin obstáculos.

## Shell (terminal, consola)

Un shell de UNIX es una interfaz de usuario de línea de comandos tradicional para sistemas operativos UNIX y GNU/Linux. Los shells más comunes son sh y bash.

## Smartphone (teléfono inteligente)

Un smartphone es un teléfono móvil que ofrece capacidades de conectividad y computación más avanzadas que cualquier teléfono móvil común contemporáneo, tales como acceso web, capacidad de ejecución de sistemas operativos elaborados y de aplicaciones integradas.

## SOCKS

Un proxy socks es una clase especial de servidor proxy. En el modelo OSI opera entre las capas de aplicación y de transporte. El puerto estándar para un proxy SOCKS es 1080, pero puede correr en otros. Algunos programas soportan una conexión a través de un proxy SOCKS. Otra opción es instalar un cliente como FreeCap, ProxyCap o SocksCap los cuales pueden forzar a los programas a correr a través de un proxy Socks usando reenvío por puerto dinámico. También es posible utilizar herramientas SSH tales como OpenSSH como un servidor proxy SOCKS.

## Software de cadena de claves

vea *administración de contraseñas*

---

## Spam

El spam son los mensajes que saturan a un canal de comunicación utilizado por la gente, sobre todo con publicidad comercial, enviados a un gran número de individuos o a grupos de discusión. La mayoría del spam anuncia productos o servicios que son ilegales en una o más formas, casi siempre incluyendo el fraude. El filtrado de contenidos de correos electrónicos para bloquear el spam, con el permiso del destinatario, es una práctica universalmente extendida.

## SSH (shell seguro)

El SSH o shell seguro es un protocolo de red que permite las comunicaciones cifradas entre computadoras. Se inventó para suceder al protocolo sin cifrado Telnet, usado para acceder a un shell en un servidor remoto.

El puerto estándar SSH es el puerto 22. Puede ser usado para eludir la censura en Internet con el reenvío de puertos o como túnel de otros programas tales como VNC.

## SSL (Secure Sockets Layer, *capa de conexión segura*)

SSL (o Secure Sockets Layer), es un estándar de cifrado usado para realizar transacciones seguras en Internet. Es la base sobre la cual se creó el TLS (Transport Layer Security, *capa de transporte segura*). Puede averiguar fácilmente si está usando SSL observando la URL en su navegador web (por ejemplo Firefox o Internet Explorer): si comienza con https en lugar de http, su conexión está cifrada.

## Subdominio

Un subdominio es una parte de un dominio mayor. Por ejemplo, “wikipedia.org” es el dominio de Wikipedia, “es.wikipedia.org” es el subdominio de la versión en español de Wikipedia.

## Texto plano

El texto plano es un texto sin formato que consiste en una secuencia de códigos de caracteres, como en ASCII o en Unicode.

## Texto sin formato

El texto sin formato es texto sin cifrar, o texto descifrado.

vea también *cifrado, TLS/SSL, SSH*.

## TLS (Seguridad en capa de transporte)

TLS es un estándar de cifrado basado en SSL, usado para realizar transacciones seguras en Internet.

## TCP/IP (Protocolo de control de transmisión sobre protocolo de Internet)

TCP e IP son los protocolos fundamentales de Internet, ya que manejan la transmisión de paquetes y su ruteo. Existen algunas

---

pocos protocolos alternativos para ser usados en este nivel de estructura de Internet, por ejemplo UDP.

## Túnel

Un túnel es una ruta alternativa desde una computadora a otra, generalmente incluye un protocolo que especifica el cifrado de los mensajes.

## Túnel DNS

Un túnel DNS es una forma de túnel a través de servidores de nombres DNS.

Debido a que “abusa” del sistema de DNS para un propósito deseado, sólo se permite una conexión muy lenta de aproximadamente 3 kbs/s que es incluso menor que la velocidad de un módem analógico. Eso no es suficiente para YouTube o para compartir archivos, pero debería ser suficiente para la mensajería instantánea como ICQ o MSN Messenger y también para el texto sin formato del correo electrónico.

En la conexión que desea utilizar un túnel de DNS, sólo tiene el puerto 53 disponible, pero aún funciona en muchos proveedores comerciales de Wi-fi sin necesidad de pagar.

El problema principal es que no hay servidores de nombres públicos modificados que se puedan utilizar. Usted tiene que configurar su cuenta. Usted necesita un servidor con una conexión permanente a Internet con Linux. Allí puede instalar el software libre *ozymandns* y en combinación con SSH y un proxy como Squid puede utilizar el túnel. Más información sobre esto en <http://www.dnstunnel.de>.

## **UDP (Paquete de datagramas de usuario)**

UDP es un protocolo alternativo usado con IP. Se puede acceder a la mayoría de los servicios de Internet usando TCP o UDP, pero existen algunos servicios que están definidos para usar exclusivamente alguno de los dos. Se usa habitualmente UDP en aplicaciones multimedia en tiempo real tales como llamadas telefónicas en Internet (VoIP).

## **URL (localizador uniforme de recursos)**

La URL es la dirección del sitio web. Por ejemplo, la URL para la sección de noticias internacionales del periódico New York Times es <http://www.nytimes.com/pages/world/index.html>. Muchos sistemas de censura pueden bloquear una URL simple. Algunas formas sencillas de eludir el bloqueo es oscureciendo a la URL. Una manera de hacerlo es agregando un punto al final del nombre del sitio, entonces la URL <http://en.cship.org/wiki/URL> se convierte en <http://en.cship.org./wiki/URL>. ; si tiene suerte con este truco podrá acceder a sitios bloqueados.

## **Usenet**

Usenet es un sistema de foros de discusión de más de 20 años de antigüedad al que se accede mediante el protocolo NNTP. Los mensajes no se almacenan en un servidor pero se encuentran en muchos servidores que distribuyen su contenido constantemente. Debido a esto es imposible censurar Usenet como un todo, no obstante el acceso a Usenet puede y se bloquea a menudo, y

---

cualquier servidor en particular es probable que lleve sólo un subconjunto de grupos de noticias de Usenet localmente aceptables. Existen archivos de Google con toda la historia disponible de mensajes de Usenet para su búsqueda.

## **VoIP (Protocolo de voz sobre Internet)**

VoIP se refiere a uno de varios protocolos para comunicación entre dos voces en tiempo real en Internet, que es notoriamente más barata que la llamada entre redes de voz de compañías telefónicas estándares. Una ventaja es que no pueden ser objeto de escuchas telefónicas como las practicadas en la telefonía tradicional, pero pueden ser monitoreadas usando tecnología digital. Muchas compañías producen software y equipamiento para espiar llamadas VoIP; las tecnologías de VoIP cifrado y seguro recién se están desarrollando.

## **VPN (red privada virtual)**

Una VPN es una red de comunicación privada usada por muchas empresas y organizaciones para conectarse en forma segura sobre una red pública. Generalmente está cifrada y nadie, excepto los extremos de la comunicación pueden ver el tráfico de datos. Existen varios estándares tales como IPSec, SSL, TLS. El uso de un proveedor de VPN es un método muy rápido, seguro y conveniente para eludir la censura en Internet con bajo riesgo pero generalmente tiene un costo mensual. Sin embargo, tenga en cuenta que el estándar PPTP no es considerado muy seguro, por lo cual se desaconseja su uso.

## Webmail

Webmail es un servicio a través de un sitio web. El servicio envía y recibe los mensajes de correo para los usuarios de la manera habitual, pero suministra una interfaz web para leer y administrar mensajes, como una alternativa al uso de un cliente de correo tal como Outlook Express o Thunderbird en la computadora del usuario. Por ejemplo, un popular servicio de webmail libre es <https://mail.google.com/>

## WHOIS

WHOIS (who is, ¿quién es?) es la función de Internet que permite realizar consultas a bases de datos WHOIS remotas para obtener información de registro de dominios. Mediante la realización de una simple búsqueda WHOIS puede descubrir cuándo y quién ha registrado un dominio, información de contacto y más.

Una búsqueda WHOIS también puede revelar el nombre o la red mapeada a una dirección IP numérica.

## World Wide Web (WWW)

La World Wide Web es la red de dominios y páginas de contenido con hipervínculos accesibles usando el protocolo de transferencia de hipertexto y sus numerosas extensiones. La World Wide Web es la parte más famosa de Internet. La necesidad del Open Source =====

Los últimos 20 años han visto un inserción de las tecnologías de redes cada vez más profunda en nuestras vidas, informando la

---

forma de comunicarnos y de actuar en el mundo. Esto acarrea algunos riesgos: cuanto menos sepamos acerca del entorno de red del cual dependemos, más vulnerables somos a la explotación.

Esta ignorancia es algo que tradicionalmente aprovechan los criminales. En los últimos años, sin embargo, algunas empresas y gobiernos se han aprovechado de la ignorancia civil en la búsqueda de un mayor control. Este flagrante y a menudo encubierto ataque a la dignidad afecta a muchos derechos básicos, y en particular, al derecho a la intimidad.

El software de código cerrado ha sido una gran bendición para esa explotación - principalmente debido al hecho de que no hay código abierto disponible para que la comunidad pueda auditar la seguridad en forma descentralizada. Bajo la premisa de proteger secretos comerciales, los desarrolladores de software de código cerrado han demostrado no estar dispuestos a explicar a los usuarios cómo trabajan sus programas. Esto puede que no sea siempre un problema si no fuera por los altos riesgos: el robo de identidad, la distribución de opiniones y sentimientos profundamente personales, los intereses de diferentes personas e incluso su casa cada vez más entran en contacto directo con el software en una contexto de redes mundiales. Muchas personas usan software con propósitos personales con la plena confianza de que es seguro. El sistema operativo Windows en sí es el más obvio ejemplo del mundo real. OS X de Apple lo sigue de cerca, con un gran porcentaje del funcionamiento interno del sistema operativo excluido de la inspección pública.

En criptografía existe un principio poderoso, establecido en el siglo 19 por *Auguste Kerckhoff* que estipula que

“[el método de cifrado] no debe exigirse que sea secreto, y debe ser capaz de caer en manos del enemigo sin inconvenientes”.

Mientras este principio ha sido llevado lejos por la mayoría de los

científicos y (por supuesto) las comunidades de código abierto - mediante la publicación de sus métodos y su funcionamiento interno, por lo que las posibles deficiencias pueden señalarse y corregirse previamente a su distribución - la mayoría de los distribuidores de software propietario dependen del secreto para ocultar las debilidades de su software. De hecho, a menudo tratan las vulnerabilidades recientemente descubiertas de una manera poco transparente - dejando a muchos usuarios confiados expuestos a ser explotados.

Por supuesto, hay que decir que el software de código abierto es tan seguro como usted lo pueda hacer (y existe gran cantidad de software de código abierto escrito por principiantes). Sin embargo, hay muchos buenos ejemplos de código bien escrito, programas bien administrados que tienen una gran (y preocupada) base de usuarios que encuentran y resuelven incluso el más pequeño de los errores rápidamente. Este es especialmente el caso del software que depende de un contexto de red.

Utilizar software de código cerrado en un contexto de red no es sólo ser parte de una minoría, significa excluirse de una amplia comunidad de investigadores y especialistas interesados en su privacidad y en su seguridad.

Nótese bien que existe una opinión más cínica del software de código abierto, que señala que, dado que nadie es pagado a tiempo completo para llevar a cabo una constante revisión y prueba de regresión, los últimos retoques de los programadores inexpertos o maliciosos podrían provocar importantes fallas de seguridad que no son detectadas por largos períodos de tiempo, dejándolo vulnerable a los hackers, criminales, agencias de inteligencia,etc. - por ejemplo, el problema (ahora resuelto) del generador de números aleatorios predecibles de Debian GNU/Linux que dio lugar a la creación de muchas claves criptográficas débiles -.

# 51

## La necesidad del software libre (o por qué es preferible al open source)

¿Por qué usar software libre? El software libre se podría definir como todos aquellos programas informáticos que respetan las cuatro libertades fundamentales de los usuarios, a saber: *La libertad de ejecutar el programa para cualquier propósito* (libertad 0). *La libertad de estudiar cómo funciona el programa, y cambiarlo para que haga lo que usted quiera* (libertad 1). El acceso al código fuente es una condición necesaria para ello. *La libertad de redistribuir copias para ayudar a su próximo* (libertad 2). *La libertad de distribuir copias de sus versiones modificadas a terceros* (libertad 3). Esto le permite ofrecer a toda la comunidad la oportunidad de beneficiarse de las modificaciones. El acceso al código fuente es una condición necesaria para ello.

Como bien puede ver, el eje principal es la libertad de los usuarios. En el momento en que los programadores liberan su software con licencias libres, el mismo deja de pertenecerles, pasando a la comunidad. Lo que importa es el propósito

de los usuarios, no el de los programadores. La importancia del software libre es que promueve la solidaridad social: compartir y cooperar. La importancia de estas libertades aumenta a medida que nuestra cultura y nuestras actividades cotidianas se vinculan cada vez más con el mundo digital. El software libre se vuelve cada vez más esencial para la libertad en general.

Aunque no era su propósito inicial, la expresión *open source*, o «código abierto» fue rápidamente asociada con ideas y argumentaciones basadas únicamente en valores de orden práctico, tales como desarrollar o usar software potente y confiable. La mayoría de los partidarios del «código abierto» llegaron al movimiento después de entonces y hacen la misma asociación de conceptos. Este criterio práctico es aceptado por la inmensa mayoría de los partidarios del open source.

En lo que respecta al software en sí mismo, tanto el software libre como el open source describen prácticamente lo mismo, entonces, ¿por qué es preferible el software libre?. El open source es pragmatismo en acción, aplicado a la programación. El software libre es un movimiento social, de profundas raíces éticas. Bueno, en este punto usted podría decir ¿y a mí qué me importa?.. lo que me interesa es el software, no la política ni nada por el estilo. Esbozaremos una respuesta...

Primero y principal, todo el software libre es software open source pero lo inverso no es cierto. Existen algunos programas (afortunadamente muy pocos) con licencia open source que no son software libre. Esto significa que los usuarios no tienen la posibilidad de disponer de ellos libremente.

En segundo lugar, muchos productos que funcionan como computadoras (por ejemplo, muchos dispositivos Android) contienen programas ejecutables cuyo código fuente es software libre, pero los dispositivos no permiten que el usuario instale versiones modificadas de esos ejecutables, es una empresa específica la que tiene el poder de modificarlos. El usuario no

---

es libre de elegir qué aplicaciones ejecutar. A esta práctica se la denomina «tivoización», con referencia al producto donde por primera vez se descubrió esta implementación. Aunque el código fuente sea libre, estos ejecutables no lo son. Segundo los criterios del código abierto, esto no es un problema; sólo les interesa la licencia del código fuente. Al centrar su atención exclusivamente en el código, no pueden apreciar estas nuevas amenazas a la libertad de los usuarios, ya que se olvida del hardware.., con lo cual estamos en una situación potencialmente muy peligrosa, es decir, si nos enfocamos únicamente en el valor práctico... ¿para qué nos sirve tener acceso al código si no disponemos de dispositivos en dónde ejecutarlos? En este punto yo lo interrogo a usted, estimado lector: ¿no le parece que *mirar para otro lado*, tratando de olvidarnos de toda cuestión *filosófica* para concentrarnos únicamente en la practicidad del uso no es un bumerán que se le volverá en contra...?

Tercero, y para finalizar, el omitir hablar de ética y de libertad, mencionando únicamente los beneficios prácticos inmediatos, para «vender» el software más fácilmente a ciertos usuarios, especialmente a las empresas, puede ser contraproducente. Si sólo se valoran los aspectos técnicos, como la confiabilidad y la potencia de un programa, se habla de una manera superficial, puramente práctica. Y acá está el germen de la autodestrucción. Si no se enseña a la gente a valorar y respetar su libertad..¿cómo pretender que la defienda?...El software libre es una cuestión de LIBERTAD, no de conveniencia.